Administration Guide

Security Awareness and Training Service 22.4.1

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

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 05, 2022
Security Awareness and Training Service 22.4.1 Administration Guide
76-224-848325-20221005

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-10-05	Initial release.

Introduction

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 threats, such as phishing, social engineering, and ransomware attacks, and provides tips on how to protect themselves and their company.

The Service also provides the customer with the ability to manage and track employee training progress via 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.

Supported Languages

The Fortinet Security Awareness and Training Service is currently supported in multiple languages.

The Admin App is available in:

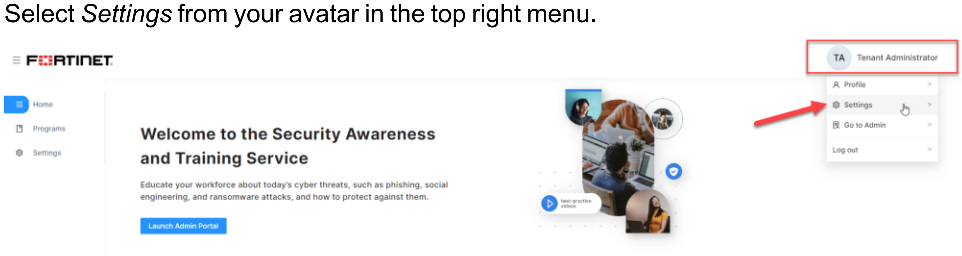
- English

The Student App is currently available in:

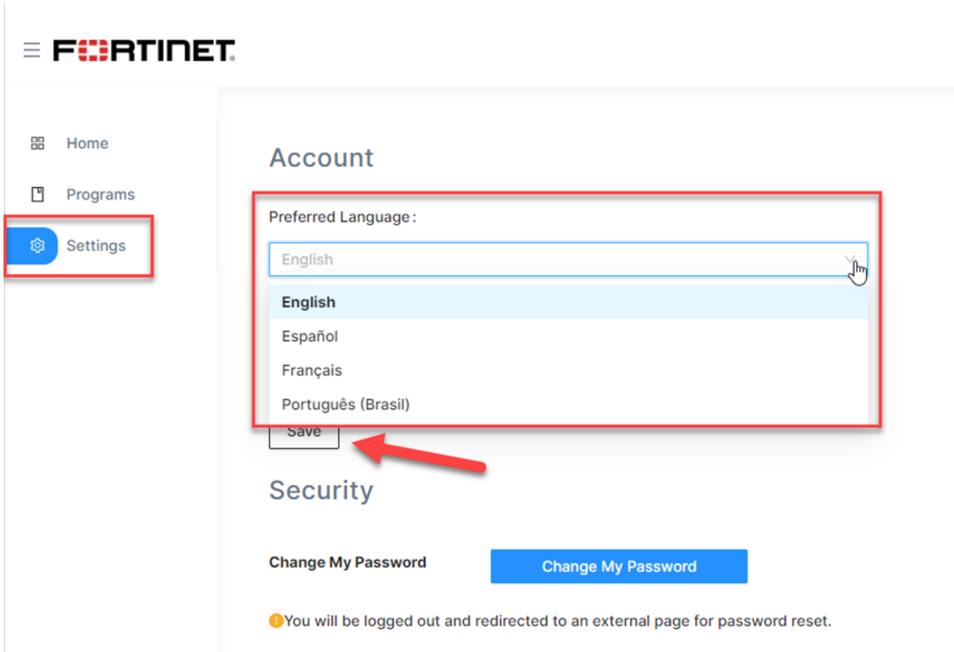
- English
- French
- Spanish
- Brazilian Portuguese

To change the language from the Student App:

1. Select *Settings* from your avatar in the top right menu.



2. Click the *Preferred Language* dropdown menu. A list of available languages is displayed.



3. Select a language.
4. Click *Save*.

Settings can also be accessed by clicking the icon in the navigation menu.

Technical support

Technical support is available for:

- 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

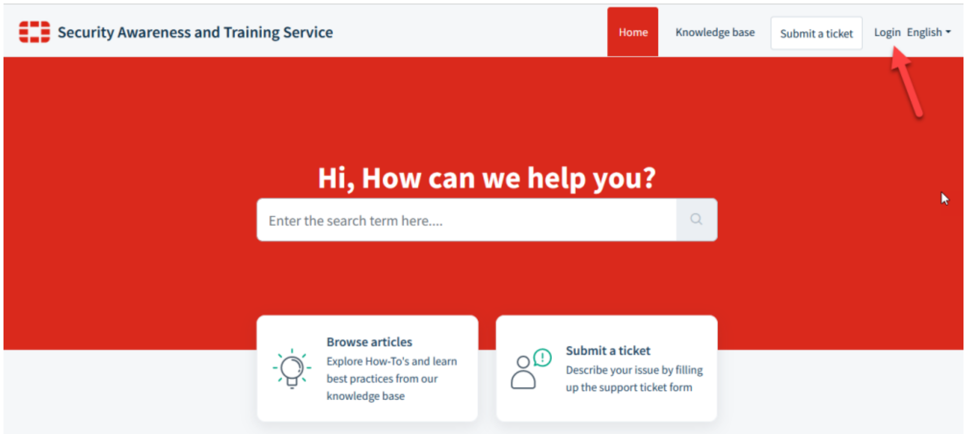
Administrators can open technical support tickets by:

- Using the *Get Support* icon
- Opening a support case by sending an email to infosec_awareness@fortinet.com.

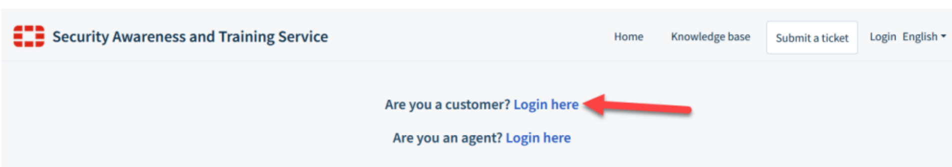
To open a technical support ticket with the Get Support icon:

1. From the user avatar in the upper right-hand corner of the screen, select the *Get Support* icon. The Security Awareness and Training Service support site opens.

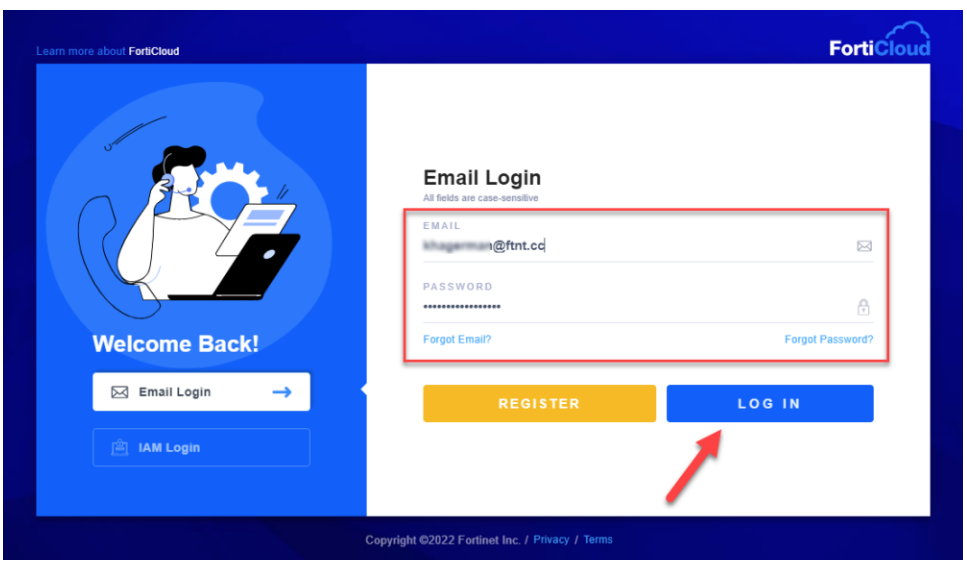
2. Once the support site has been loaded, select *Login*.



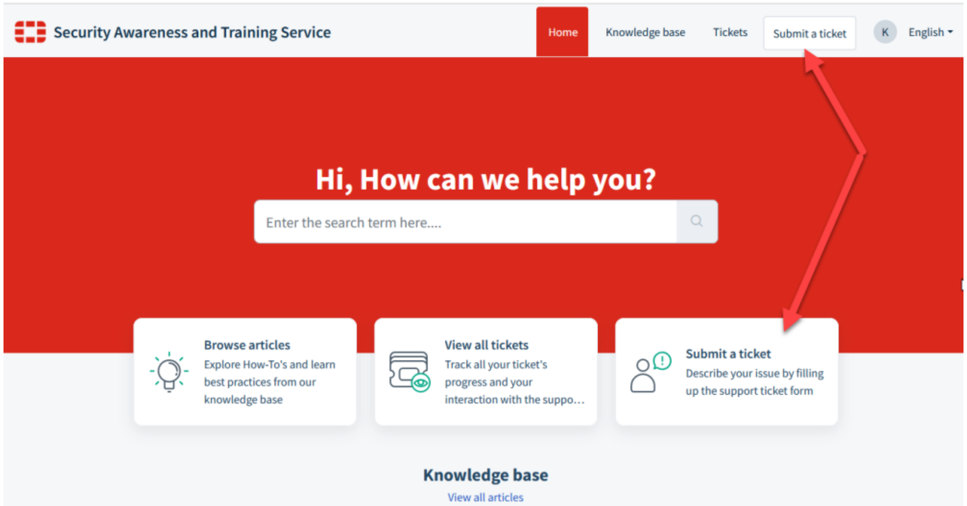
3. Select *Are you a customer? Login here*.



4. Log in with your FortiCloud Support credentials. These are the same credentials you use to log in to the service.

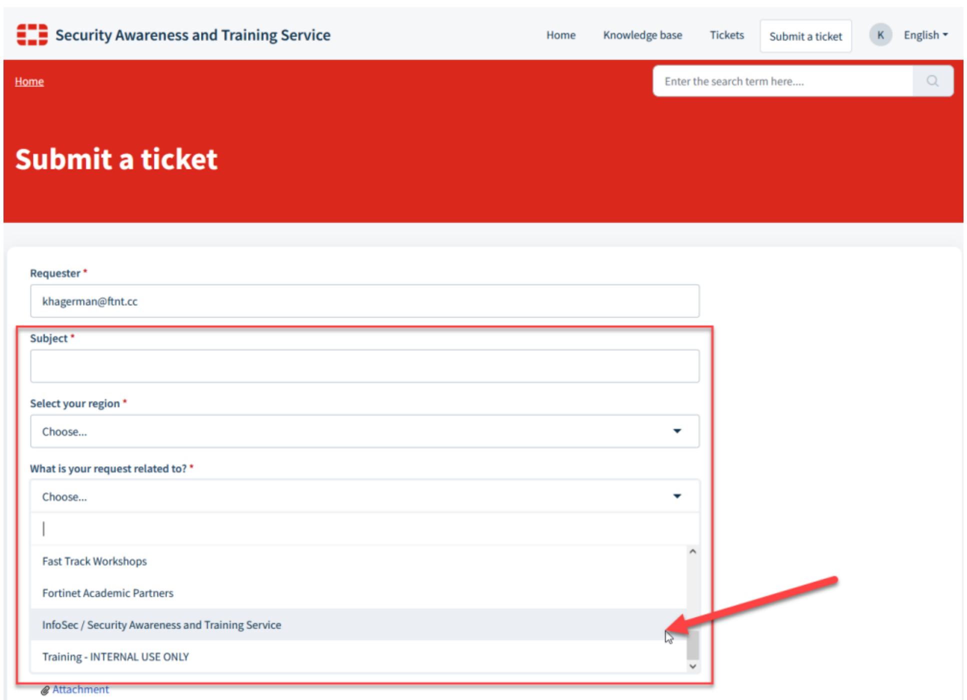


5. Select *Submit a ticket*.



6. Complete the fields in the form:

Subject	Provide a brief description of the question or issue being face.
Select your region	Select the region of the Administrator opening the ticket.
What is your request related to?	Select *Infosec/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 of issue, including steps to reproduce the issue, screen shots, browser builds, and so on.
Attach a file	Include any files you wish to submit with the ticket.



7. 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.

Only Administrators of the systems can open cases with support.

Students should report any issues or raise any questions or feature requests to their Administrator. The Administrator should open a case with Support using the email above.

You will receive a confirmation email of the submission.

A Deployment Specialist will follow up on the newly created ticket thread.

Best Practices

When opening a support ticket via email, ensure 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
- Operating System and version (if applicable)
- Browser and version (if applicable)

Please raise one question, issue, or feature request per ticket.

Please do not raise new queries on existing or older (closed/resolved) tickets.

Key users

There are three key user types:

- Administrator
- Partner
- Student

Administrator (Customer or Partner)

The Administrator will serve as a single point of contact for liaising with the Fortinet Training Institute for the duration of the service and must have executive sponsorship within their company to act as their Security Awareness and Training Service Administrator.

The Administrator user is the super user of the SAT (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.

Each customer has a tenant. The tenant is the unique instance of the Admin Portal.

There can only be one Administrator per tenant. If a Partner organization is configuring and managing the tenant, then the customer administrative account must be used by the Partner. There are instructions on configuring partner access in Account management on page 39.

Administrators can log in from the product page https://my.ftnt.info after they create a support account.

Accessing the support portal requires the customer to setup an account (if they do not have one) or, log in using their existing credentials. This allows customers to enter license strings for the system, such as Standard, Premium, and Custom brand (add-on).

Partner

If you are a Partner, once you have initialized your tenant, you must reach out to infosec_awareness@fortinet.com and request partner access to your tenant. This will allow Partner access to the following functionality:

- *Content*: All modules, micro-modules, and nano-modules
- *Domains*: For the configuration of Domains and Custom Sub Learning Domains
- *Users*: For LDAP import
- *Authentication*: For configuration of Single Sign-on (SAML2 / IdP)
- *Account Management*: Customer Account Management (add customer administrators to tenants)
- *Appearance*: For customization of appearance settings.

Once Partner access is granted, invitations can be sent to Customers via email to invite them to allow the Partner to log in as the Customer Tenant Administrator. There are instructions on configuring partner access in Account management on page 39.

Student

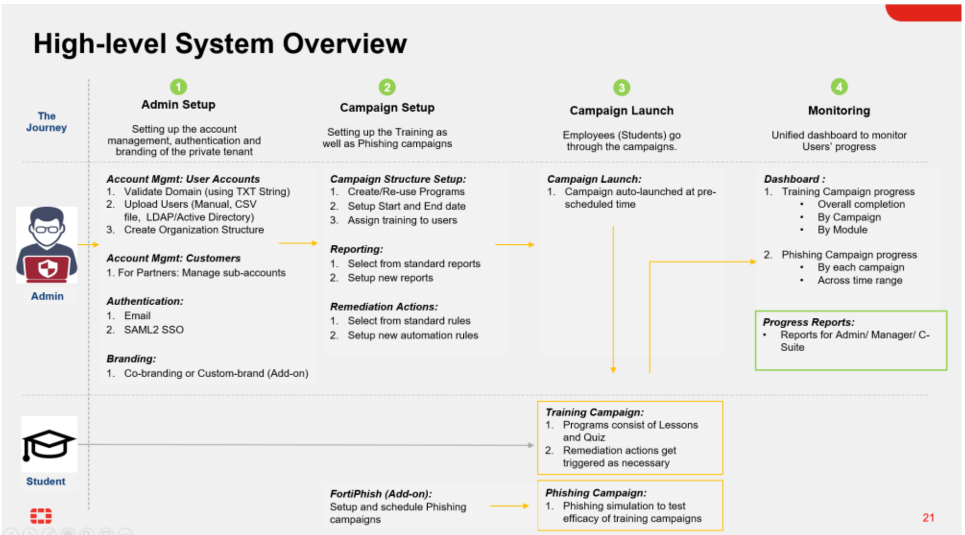
This user (usually employees) is the intended audience for the Security Awareness and Training Service. The students receive the training campaigns setup by the Administrator.

Administrators can also be a student. They select whether to access the Admin console after logging in and can toggle between the Admin and user (student) consoles.

Students can authenticate by entering their login credentials from the URL provided from their tenant Admin.

System overview

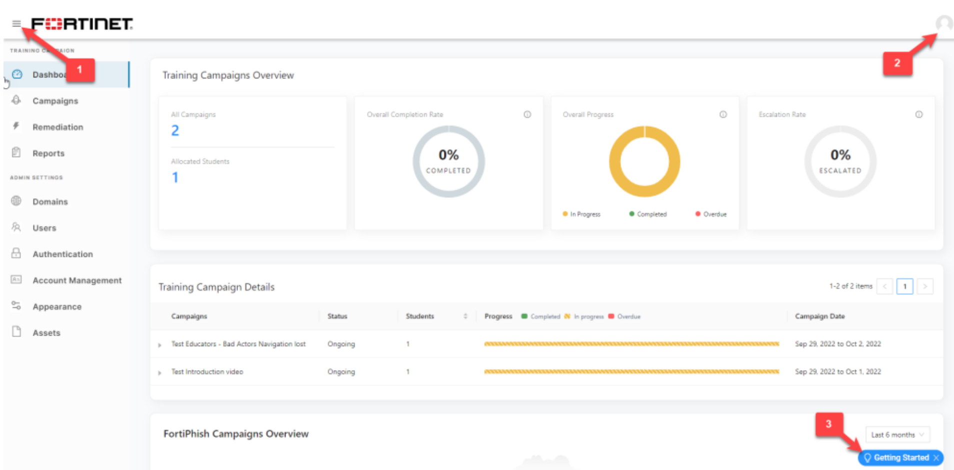
The following image present a high-level overview of all the key features organized in a logical sequence that represents the interaction points of Admin and Student with the Security Awareness and Training (SAT) Service:



Navigating the main screen

Security Awareness and Training Service resources are available from the main screen, including:

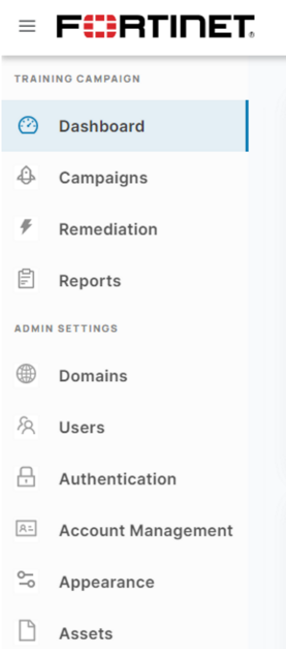
1. Navigation menu icon
2. Avatar icon
3. *Getting Started*



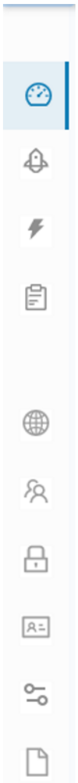
Navigation Menu

The three vertical bars in the upper left-hand corner of the screen allow you to toggle the text references next to the Navigation Menu icons. Clicking this icon will toggle the text entries to display or hide (and only show the icons).

When text entries are displayed, the Navigation Menu will appear as follows:

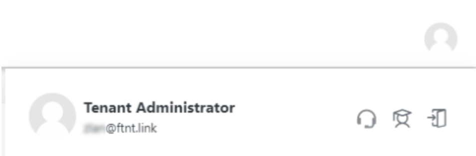


When the text entries are hidden, the Navigation Menu will appear as follows:



Avatar

The avatar icon (this may show a picture of the user, if uploaded) shows more information about the user who is currently logged in to the system.



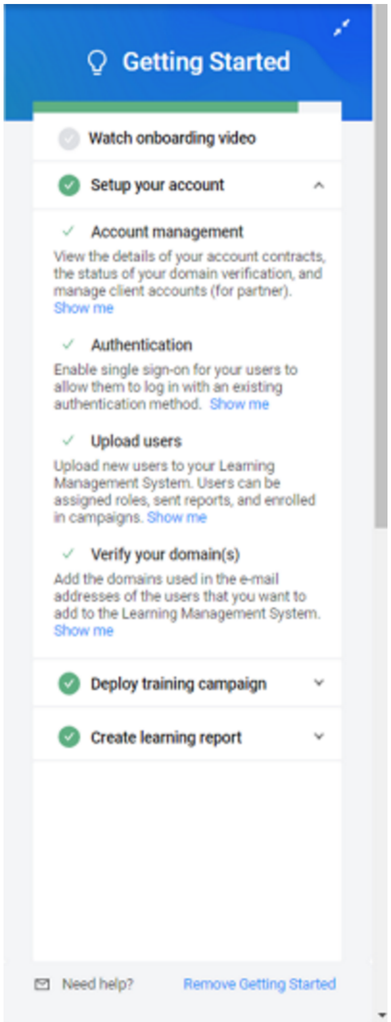
There are three icons available to the Administrator:

- *Get Support*: Clicking this icon will open a browser tab directing Administrators to the Security Awareness and Training support site. From here, Administrators can access FAQs, Knowledge Articles, and log in to the support portal to open support tickets to report problems or ask questions.
- *Go to Learning App*: Clicking this icon will take the Administrator out to the Student (Learning) App.
- *Log Out*: Clicking this icon will log out the currently logged in Administrator.

Getting Started

In the lower right corner, there is a *Getting Started* button that provides Administrators information on using the system. Topics include:

- *Watch onboarding video*
- *Setup your account*
  - *Account management*
    - View the details of your account contracts, the status of your domain verification, and manage client accounts.
  - *Authentication*
    - Enable single sign-on for your users to allow them to log in with an existing authentication method.
  - *Upload users*
    - Upload new users to your Admin Portal. Users can be assigned roles, sent reports, and enrolled in campaigns.
  - *Verify your domains*
    - Add the domains used in the e-mail addresses of the users that you want to add to the Admin Portal.
- *Deploy training campaign*
  - Create training campaigns to deploy and schedule programs, and modules for your users.
- *Create learning report*
  - *New Reports*
    - Please create a new report
- *Need Help?*
  - Send an email by opening a case using the *Need help?* link at the bottom of the *Getting Started* interface.

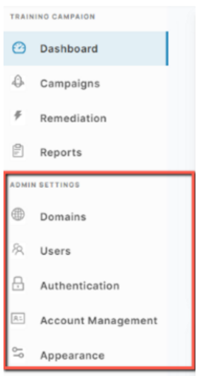


If you select the *Remove Getting Started* link, the *Getting Started* pop-up button in the lower right-hand corner of the screen is removed. To re-add it, click on the *Open Getting Started* link in the lower left-hand side of the screen.

Admin settings

This section describes the initial setup activities the Administrator needs to carry out to configure the tenancy. It includes:

- *Domain*: Configuration and validation of your domain.
- *Users*: Creating your organizational structure via uploading users (Manual creation, import from .csv, and LDAP synchronization).
- *Authentication*: Configuring SAML2 Single Sign On (SSO).
- *Account Settings*: Customer account management (for Partners to manage Customer sub-accounts).
- *Appearance*: Branding of the site, including Co-branding or Custom-brand (Add-on).

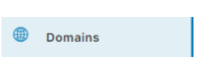


When first accessing the configuration pages, the configuration *Tour* window will appear. You can follow the tour or cancel the tour and configure the domains yourself.

This section includes the following topics:

- Domains - Configuration and validation of your domains and sub (learning) domains on page 18
- Users - Creating your organizational structure through uploading users on page 24
- Uploading users on page 25
- Authentication - Configuring SAML2 single sign on on page 36
- Account management on page 39
- Adding a customer account (Partners only) on page 40
- Appearance (Premium service only) on page 42

Domains - Configuration and validation of your domains and sub (learning) domains



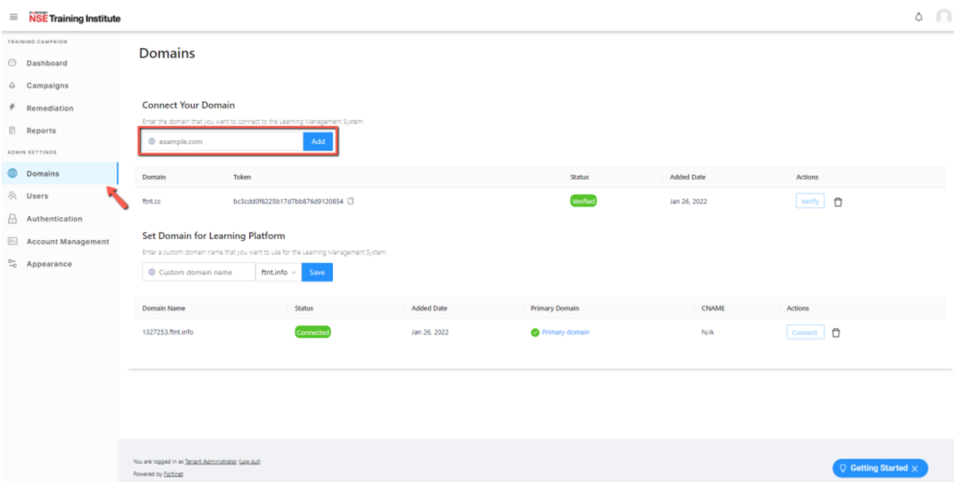
The first configuration step is to verify your domain in the Admin Portal tenant. You need to add DNS TXT records for your domain to prove ownership of your domain before uploading users and customizing your URL domain. You can only add users with email addresses that use a verified domain.

Domain names must contain:

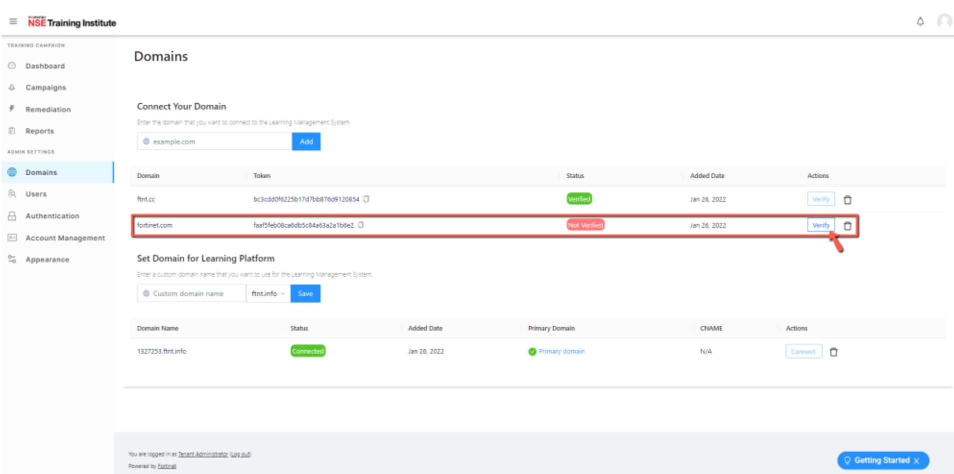
- Lowercase only
- At least one letter
- At least three characters
- No more than 64 characters
- No special characters

To configure a domain:

1. Go to *Domains*. Once selected, you can enter the parent domain in the *Connect Your Domain* field and click *Add*.



Once entered, a Token will be generated.



2. In order to complete the verification process, you must add the token generated as a DNS TXT record in your domain DNS configuration to prove that you own the domain.

   This entry may take time to propagate across the networks.

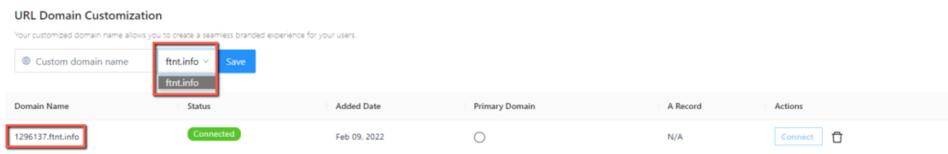
3. Once this step has been completed, click *Verify*.

This step must be completed by someone in the customer's IT department who has access to your DNS domain configuration. Fortinet cannot assist in this step or do it for the customer.

There is also trash can icon that you can click to delete the domain registration entry

URL domain customization - Unpaid (free) 25 user service

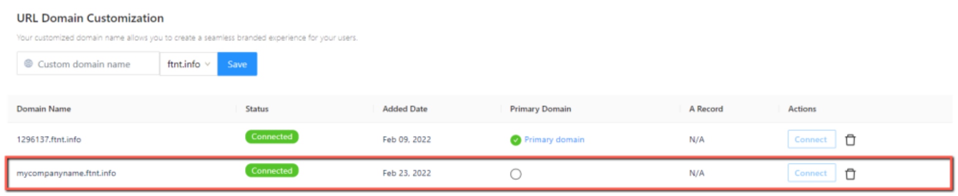
After you have finished the *Verify Domain Ownership* in the *Domains* sectio,n a default domain of *ftnt.info* will appear in the URL. Your site URL will be showed as: <*Tenant ID*>*.ftnt.info*:



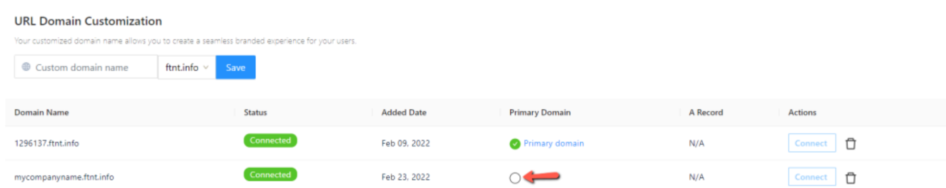
To add a new (more meaningful) subdomain:

1. Enter a new subdomain (for example, your company name) in the *Custom domain name* text box and select *Save*.

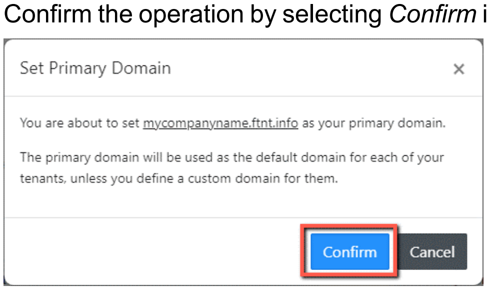
Your new custom domain will appear in the list.



2. To begin using this more meaningful subdomain, select the *Primary domain* option button.

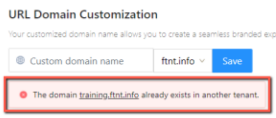


3. Confirm the operation by selecting *Confirm* in the dialog box.



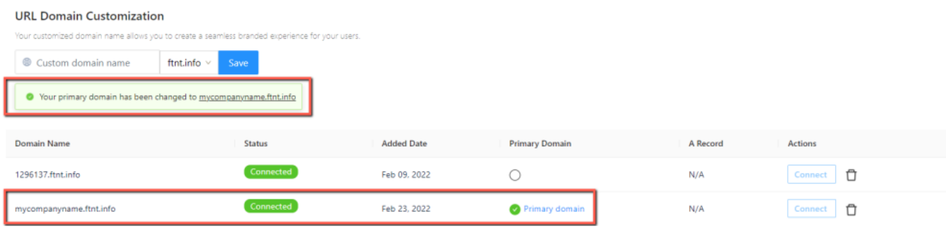
If you attempt to add a subdomain to *ftnt.info* that already exists in the system, you will receive the following error:

The domain <the domain you entered>.ftnt.info already exists in the tenant.



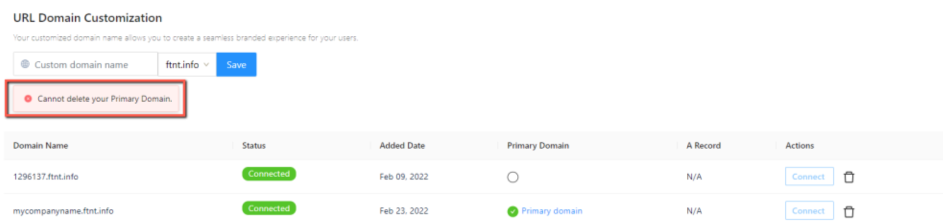
If this domain has not been used before, you will see a confirmation message:

Your primary domain has been changed to <the domain you entered>.ftnt.info



If you try to delete a *Primary domain* by clicking on the trashcan icon, you will receive the following error:

Cannot delete your Primary Domain.



You must first assign a new *Primary domain* and then perform the delete operation.

URL domain customization - Paid service offering

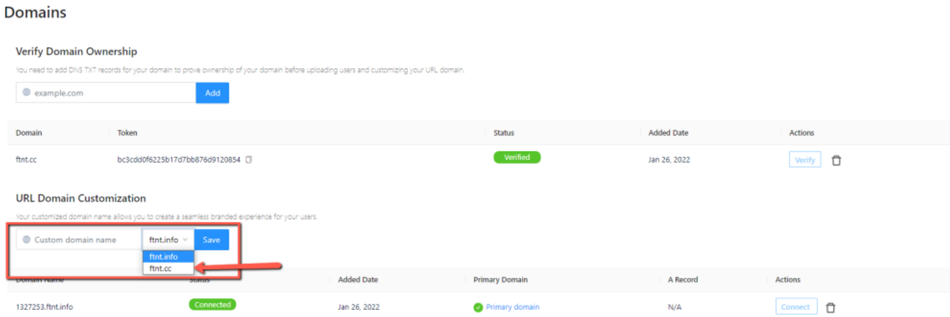
This option is not available with the free 25 user service. Users of the free service will only be able to use <tenant id>.<customer domain>.

The last step for domain configuration is to set the domain you intend to use for your Learning Platform.

Using the *URL Domain Customization* option will create a subdomain under your parent domain (e.g. mysubdomain.mydomain.topleveldomain) that your users will recognize. Once verified, the parent domain should appear in the dropdown.

To create a subdomain:

1. From the dropdown list under *URL Domain Customization*, select your domain.

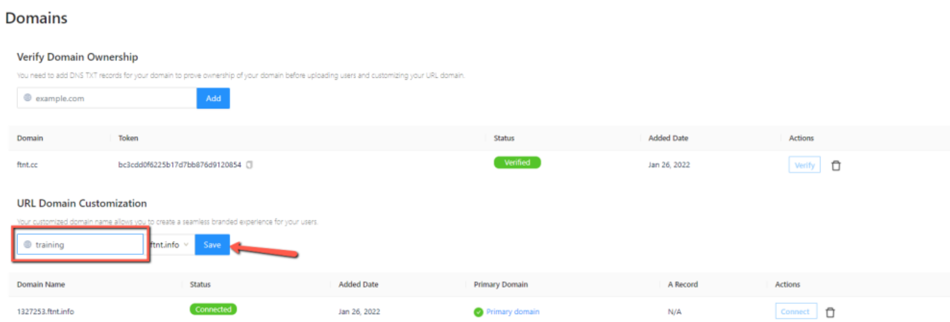


2. Enter the subdomain name and click *Save*.

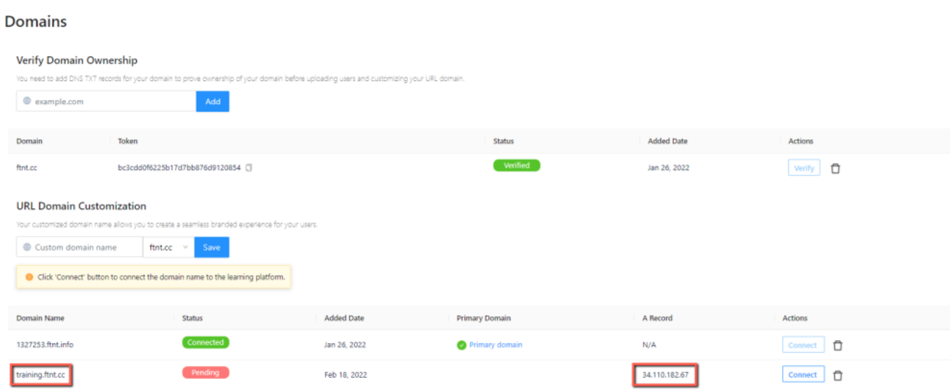
Only enter the subdomain, i.e., mysubdomain (the parent domain is picked up from the dropdown list).

Subdomain names must contain:

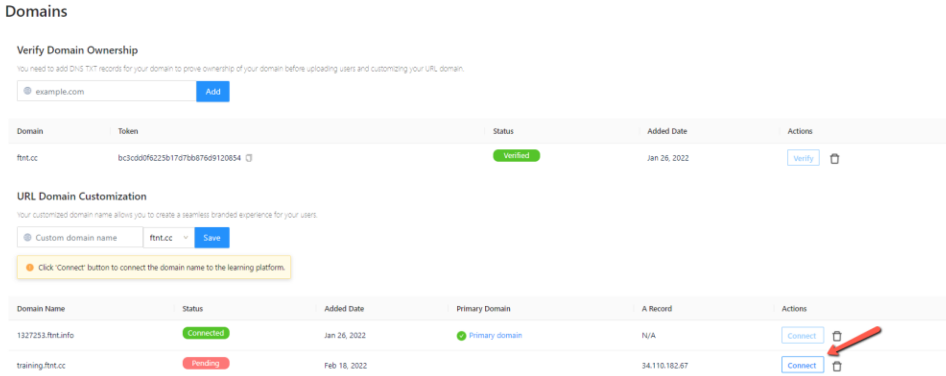
- Lowercase only
- At least one letter
- At least three characters
- No more than 64 characters
- No special characters



3. Provide the subdomain (i.e. mysubdomainname.mydomain.topleveldomain) and the IP address (under the *A Record* column) to your network administrator so that they can create an *A Record* entry under their domain. This may take time to propagate across networks. The *Status* will show as *Pending*.

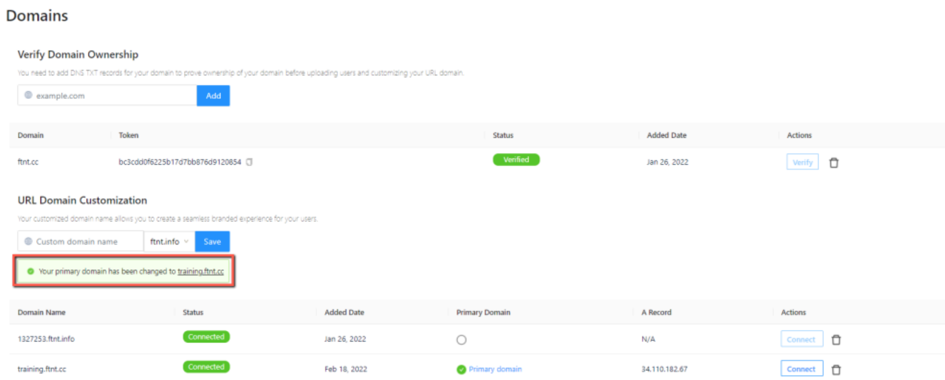


4. Once the *A Record* has been added and has propagated, click the *Connect* button.



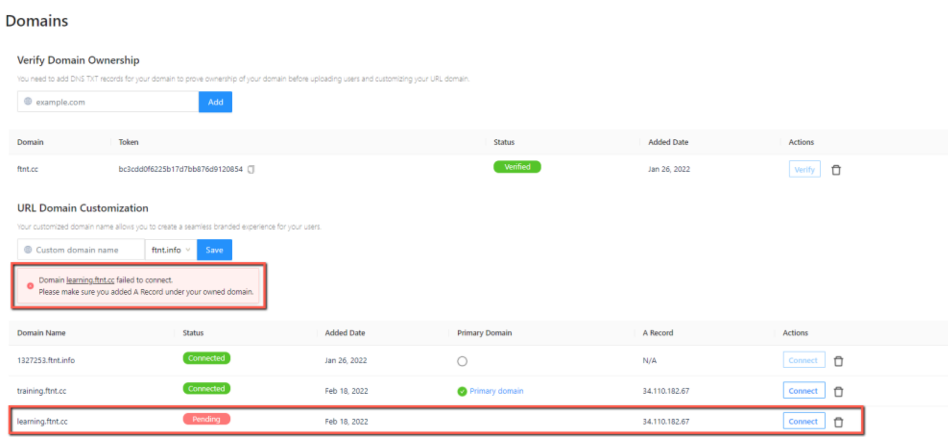
5. Now, under the *URL Domain Customization* section, select the *Primary Domain* button to change to your new subdomain to act as the primary domain for the tenant. You should see the following confirmation message:

   Your primary domain has been changed to training.ftnt.cc



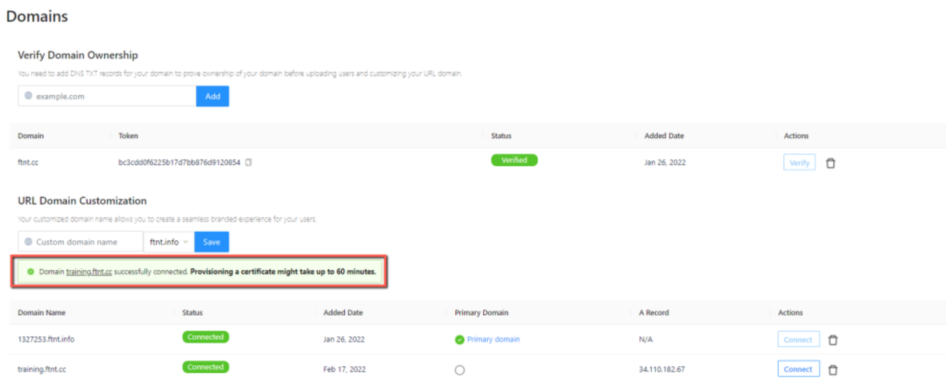
If the *A Record* has not been propagated, you will see the following error:

Domain mysubdomain.mydomain.topleveldomain failed to connect. Please make sure you added A Record under your owned domain.

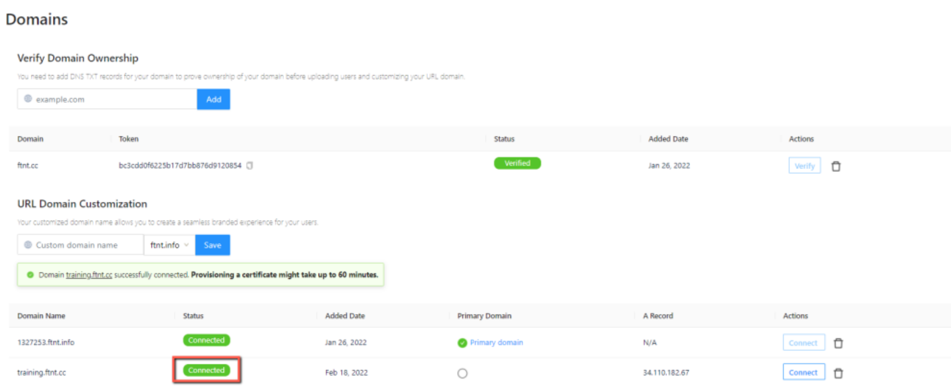


If the *A Record* has been added and successfully propagated, you will see the following notification:

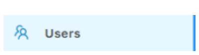
Domain secaware.ftnt.cc successfully connected. Provisioning a certificate might take up to 60 minutes.



The *Status* column should also show *Connected*.



Users - Creating your organizational structure through uploading users



Before you can create your campaign, you must first import users. Depending on which data is included during user import, an Organization Structure is created.

Organization Structure is a combination of three workplace features:

- Departments
- Title

Customers should already have their organizational structure available to them via their Active Directory or HR system. Customers can export from whichever data source they choose to use to import users from a .csv file. The complexity usually depends on the size of the organization and the geographical location of employees. This usually directs the hierarchy of their organization. Important factors that dictate the complexity of an organizational structure, likely include, but are not limited to:

- How many employees are there?
- Where are employees located (globally)?

- What is the user job functions (titles)?
- What is the reporting structure (hierarchy) of the organization?

Departments

In the Departments framework, you can refer to Departments when scheduling Campaigns, Reporting, and Dynamic Rules.

Title

Positions Frameworks and Positions work in a similar way to Departments. During the creation or import (through .csv or LDAP import), Positions are added to the system. You can refer to Positions when scheduling Campaigns, Reporting, and Dynamic Rules.

Uploading users

There are three ways that users can be added to the Admin Portal:

- Manually creating users via the tenant interface by entering the user First Name, Last Name, Email, Department, and Title.

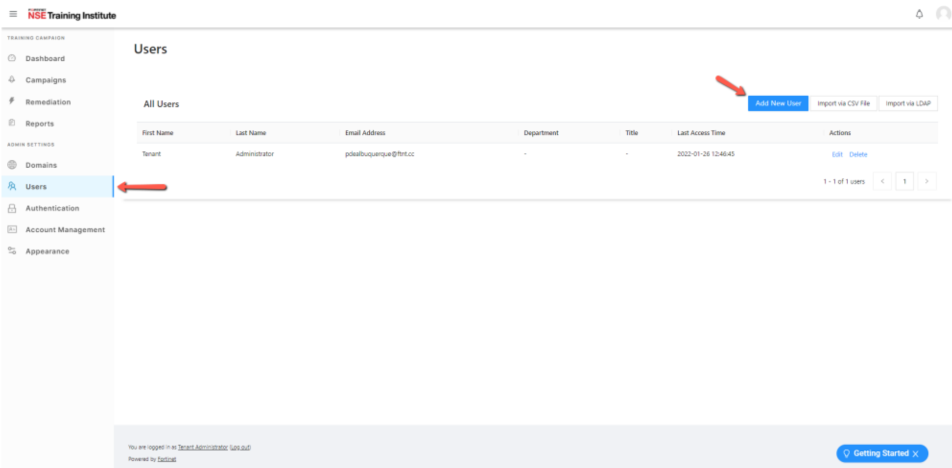
  There is no mapping to a manager email when creating users using this method. This means that managers will not receive notifications for Remediation rules.

- Importing from a CSV file which includes the user First Name, Last Name, Country, Email, Department, Job Title, and Manager email. When included in the .csv, the manager email is used to build the reporting hierarchy in the framework.
- Synchronizing from an LDAP Directory. Currently only LDAP import is available. LDAPs (LDAP with TLS) will be supported at a later date. When importing from LDAP, the Organizational Units (OU) of the Directory are used to populate the various Departments framework and the title Directory attribute is used to populate the Positions framework. The mail attribute from the user entry is used to populate the email address for the user. You should use the *givenName* attribute and *Surname* (sn) attribute, to populate the First and Last names in the tenant.

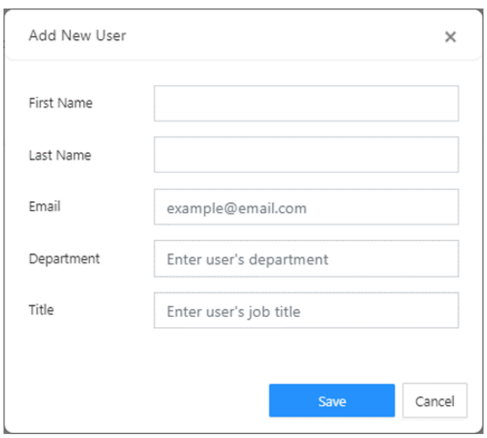
Manually Creating Users

To manually create users:

1. Go to *Users*, then select *Add New User*.



2. Enter the requested information into the *Add New User* dialog (*First Name*, *Last Name*, *Email*, *Department*, and *Title*) and select *Save*.

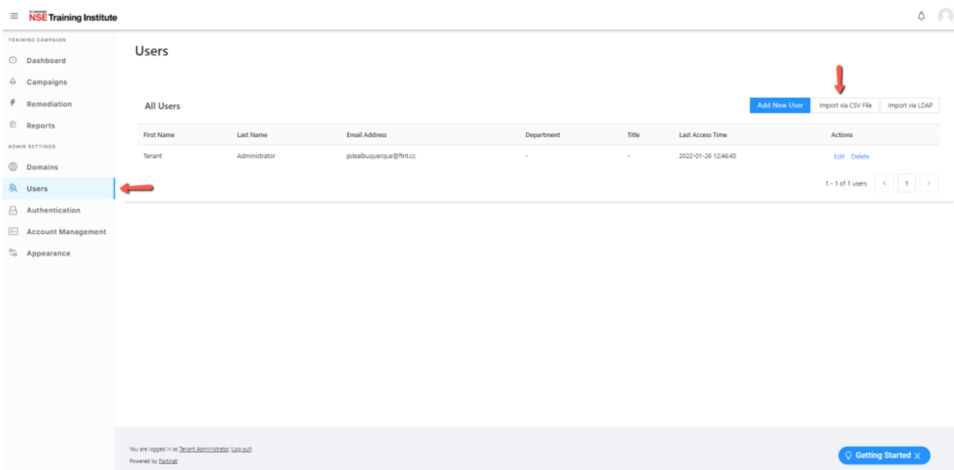


You should now be able to find the user entry in the system by selecting *Users* in the Navigation Menu.

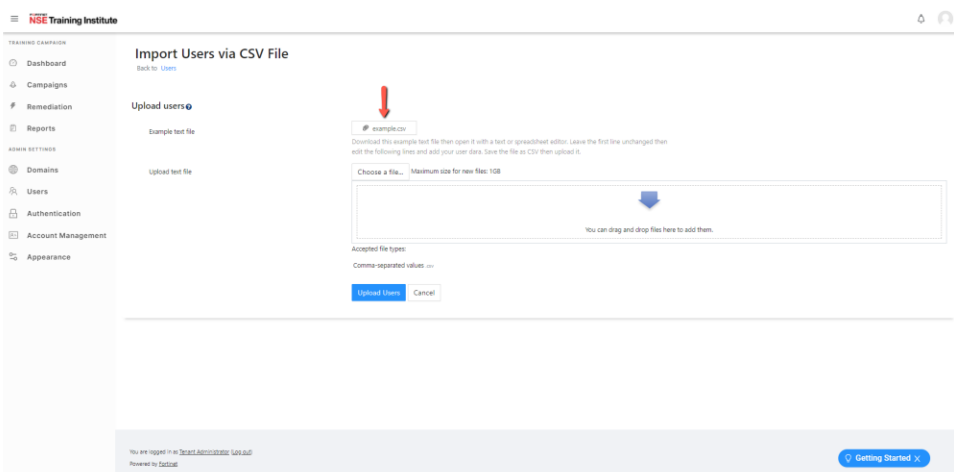
Importing from a CSV file

To import from a CSV file:

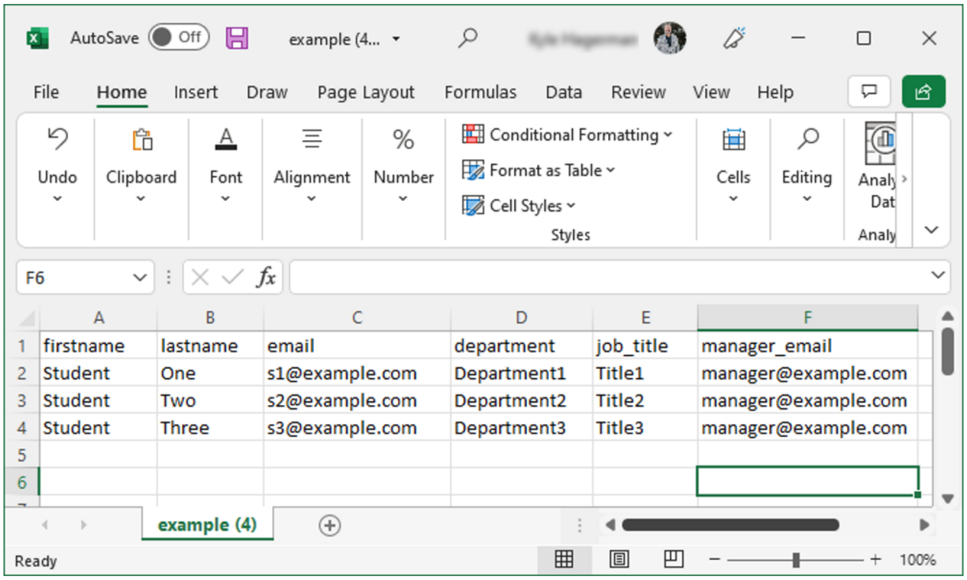
1. Go to *Users*, then select the *Import via CSV File*.



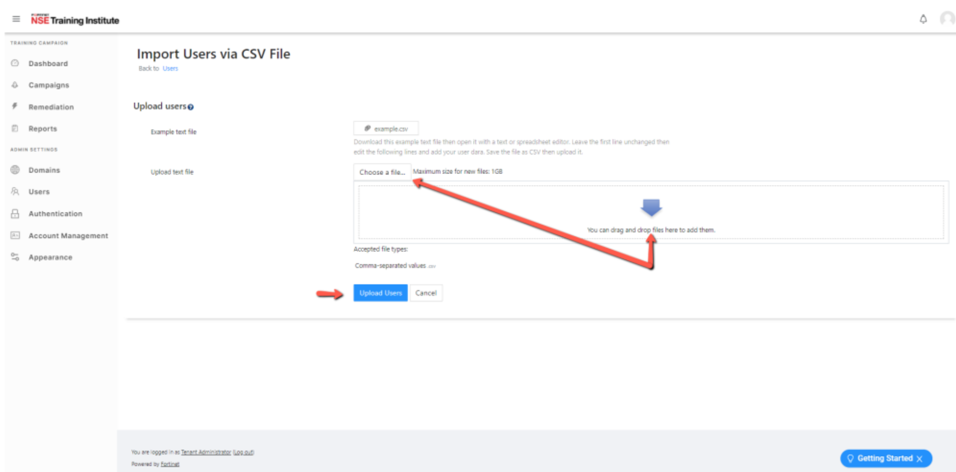
2. Before you can import users via a CSV file, you must first download the *example.csv* text file then open it with a text or spreadsheet editor.



Save the file as CSV. Once downloaded, you can open the spreadsheet to see the expected input. Leave the first line unchanged then edit the following lines and add your user data.

3. 

4. Upload the file by either dragging and dropping it into the frame, or, browsing to and choosing a file for upload.



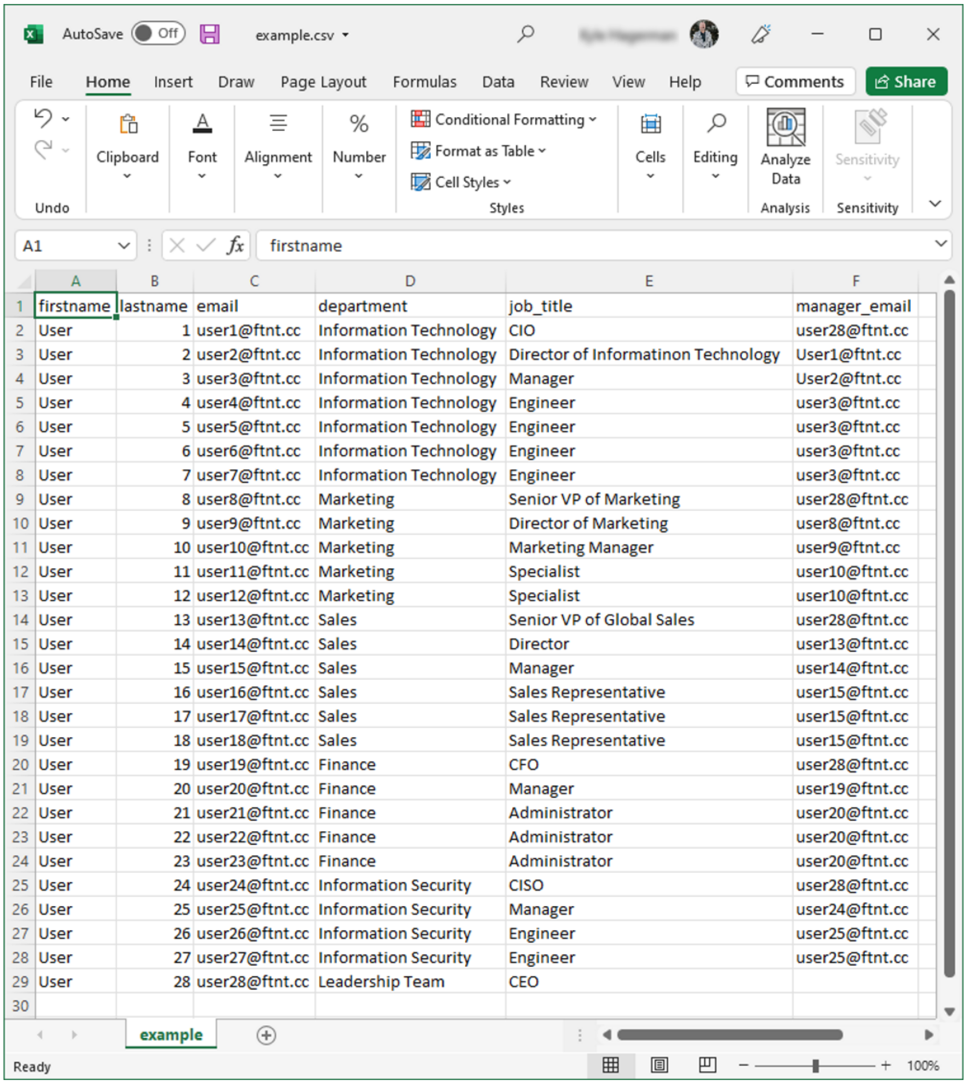
Best practices

When you are editing the CSV file, use the following best practices:

- Do not modify the first row entries values, or change their order. These are system variables that map to the tenant database.
- Ensure case sensitivity (title case) and accuracy for the *firstname*, *lastname*, *country*, *email*, *department*, *job_title*, and *manager_email*. The values entered here will be used in reporting, printed completion certificates, and so on.
- Include all data requested in the spreadsheet (First Name, Last Name, Country, Email, Department, Job Title, and Manager email). Not including the *job_title* and *manager_email* values will create a flat structure. If the manager email is not included (including the manager's entry in the .xlsx), then Remediation rules will not send emails to a manager. For example, if you do not include the Department, all users will be listed in one Department with a default name. If you do not include the *manager_email*, you will also not get a hierarchy of users making it more labor intensive to set up reporting.

Sample input when all columns are populated

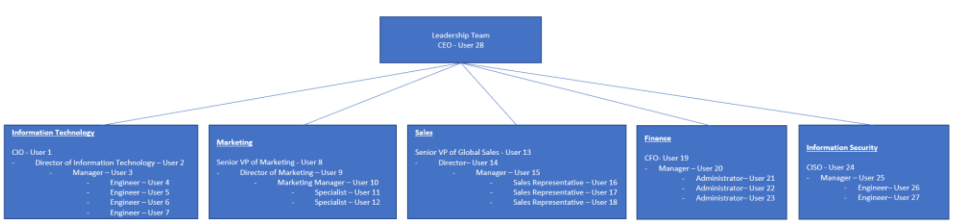
The following image includes an example file with values inputted:



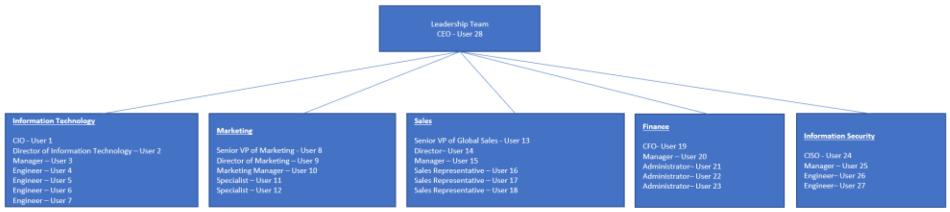
firstname	lastname	email	department	job_title	manager_email
User	1	user1@ftnt.cc	Information Technology	CIO	user28@ftnt.cc
User	2	user2@ftnt.cc	Information Technology	Director of Informatinon Technology	User1@ftnt.cc
User	3	user3@ftnt.cc	Information Technology	Manager	User2@ftnt.cc
User	4	user4@ftnt.cc	Information Technology	Engineer	user3@ftnt.cc
User	5	user5@ftnt.cc	Information Technology	Engineer	user3@ftnt.cc
User	6	user6@ftnt.cc	Information Technology	Engineer	user3@ftnt.cc
User	7	user7@ftnt.cc	Information Technology	Engineer	user3@ftnt.cc
User	8	user8@ftnt.cc	Marketing	Senior VP of Marketing	user28@ftnt.cc
User	9	user9@ftnt.cc	Marketing	Director of Marketing	user8@ftnt.cc
User	10	user10@ftnt.cc	Marketing	Marketing Manager	user9@ftnt.cc
User	11	user11@ftnt.cc	Marketing	Specialist	user10@ftnt.cc
User	12	user12@ftnt.cc	Marketing	Specialist	user10@ftnt.cc
User	13	user13@ftnt.cc	Sales	Senior VP of Global Sales	user28@ftnt.cc
User	14	user14@ftnt.cc	Sales	Director	user13@ftnt.cc
User	15	user15@ftnt.cc	Sales	Manager	user14@ftnt.cc
User	16	user16@ftnt.cc	Sales	Sales Representative	user15@ftnt.cc
User	17	user17@ftnt.cc	Sales	Sales Representative	user15@ftnt.cc
User	18	user18@ftnt.cc	Sales	Sales Representative	user15@ftnt.cc
User	19	user19@ftnt.cc	Finance	CFO	user28@ftnt.cc
User	20	user20@ftnt.cc	Finance	Manager	user19@ftnt.cc
User	21	user21@ftnt.cc	Finance	Administrator	user20@ftnt.cc
User	22	user22@ftnt.cc	Finance	Administrator	user20@ftnt.cc
User	23	user23@ftnt.cc	Finance	Administrator	user20@ftnt.cc
User	24	user24@ftnt.cc	Information Security	CISO	user28@ftnt.cc
User	25	user25@ftnt.cc	Information Security	Manager	user24@ftnt.cc
User	26	user26@ftnt.cc	Information Security	Engineer	user25@ftnt.cc
User	27	user27@ftnt.cc	Information Security	Engineer	user25@ftnt.cc
User	28	user28@ftnt.cc	Leadership Team	CEO	

In this data set, there would be five departments created in the Department framework: Information Technology, Marketing, Sales, Finance, and Information Security since these are the only unique Department framework values.

For the positions Framework, the following hierarchy would be created due to the population of the *manager_email* column:



If you chose not to include the *manager_email* column, the structure would look like the following:



Note that the Departments are still there, however, there is no hierarchical structure below the department. We can still assign one or more of the management level to receive reports, and so on when manually setting up the report.

If you choose not to include the departments column in the .csv file, your organizational structure would be flat. All users would appear in one group. For smaller organizations, this may still be okay as there may only be one or two administrators managing the Admin Portal.

Synchronizing from an LDAP Directory.

For Premium accounts, customer and partner administrators may import users from an LDAP Directory server or a Microsoft Active Directory server. If this method is used, you must map the appropriate attributes from the LDAP Directory to the correct Portal attributes.

Connectivity must be available through the firewall in order for the service to import and periodically sync users from your Directory if it is not available in the DMZ or on the internet. This may require firewall changes to your networked environment. It may also require an account to authenticate and bind to your Directory.

When creating firewall rules, open traffic from the following IPs and the port you use and configure in your LDAP server:

- 44.199.89.48
- 23.23.99.234

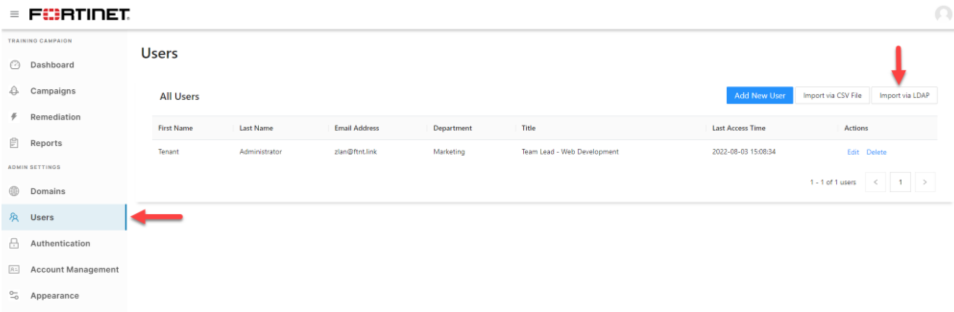
Here are the default Directory attributes. It is important that all Directory attributes are present and populated for the service to operate correctly:

Service field name	Directory attribute
Firstname	givenName
Lastname	sn
Email	mail
Title	title
Department	department
Manager	Manager This attribute maps the DN (distinguished name) of the users manager in Active Directly.

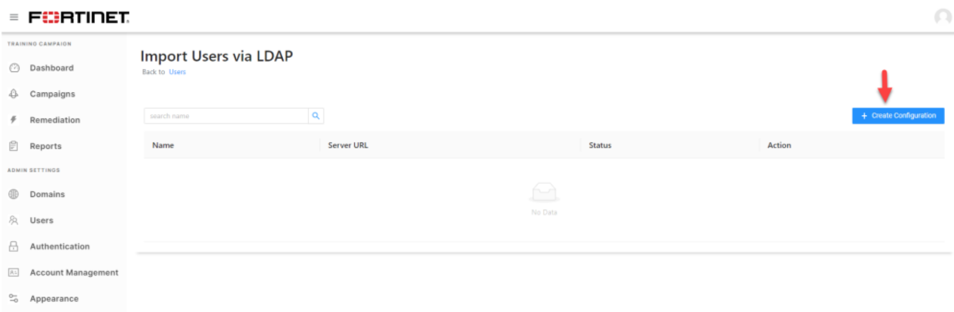
Before configuring LDAP import of users, please open a case by sending an email to infosec_awareness@fortinet.com for assistance and additional information.

To create a configuration:

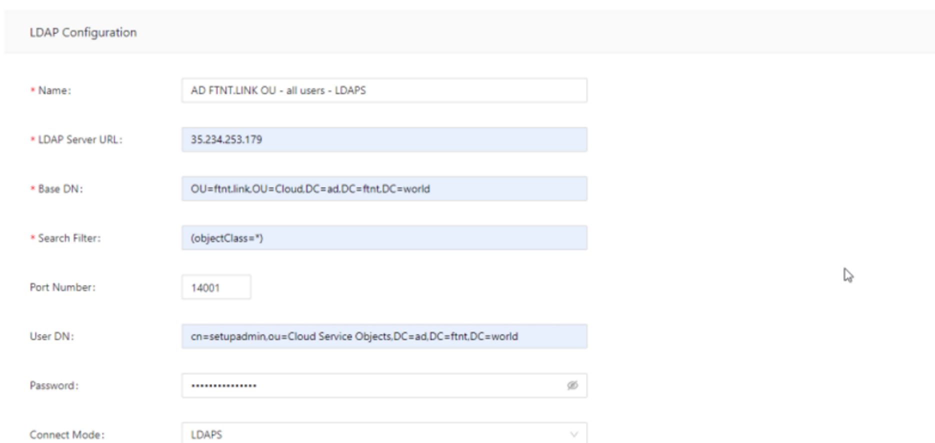
1. Go to *Users* and select *Import via LDAP*.



2. Click *Create Configuration*.



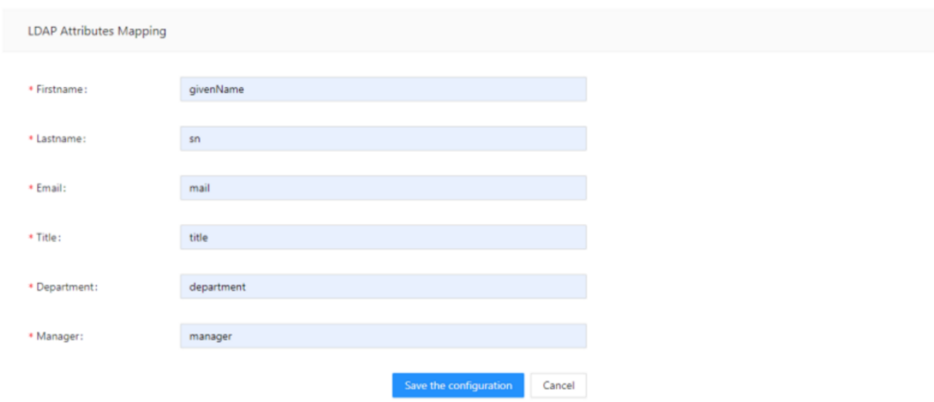
3. Configure the *LDAP Configuration* settings.



Setting	Description
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.

Setting	Description
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, 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.
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=*).
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.
User DN	Enter the Directory username that will be used to allow the service to bind to your Directory.
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).

4. Configure the *LDAP Attributes Mapping* settings.



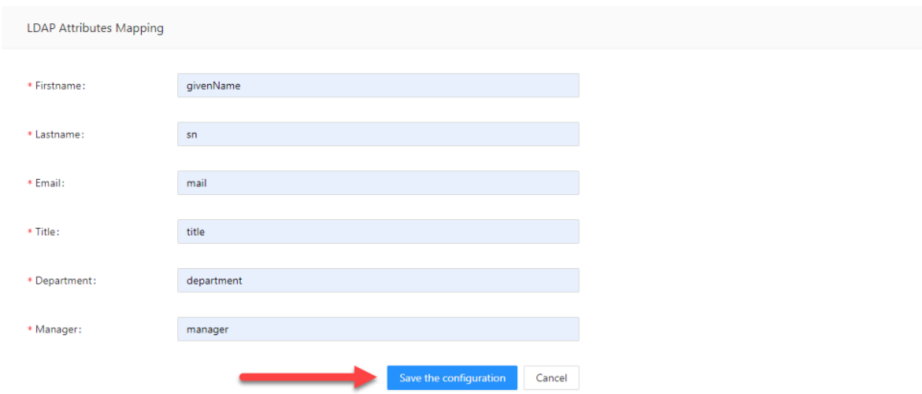
Before configuring this section, contact your Directory administrator to obtain the Directory attributes being used to store the following information. Default Directory attributes for Active Directory have been provided. All data points mentioned below should be present and populated either in the default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

Attribute names are case sensitive.

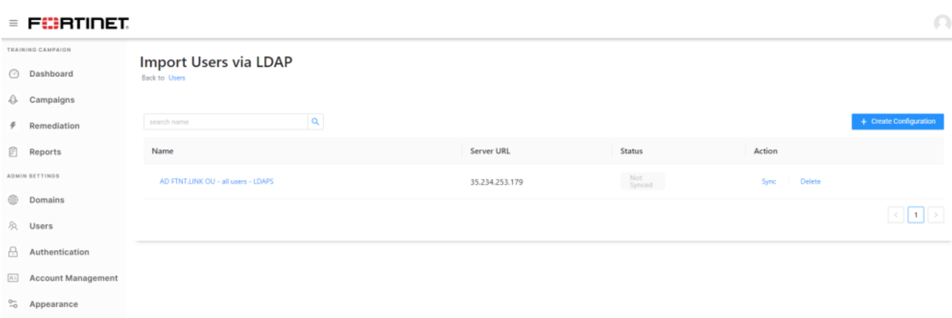
Setting	Description
Firstname	Enter the Directory attribute where the user's first name information is stored. By default, in Active Directory, this is the givenName attribute.
Lastname	Enter the Directory attribute where the user's last name information is stored.

Setting	Description
	By default, in Active Directory, this is the sn (surname) attribute.
Email	Enter the Directory attribute where the user's email information is stored. By default, in Active Directory, this is the mail attribute.
Title	Enter the Directory attribute where the user's title information is stored. By default, in Active Directory, this is the title attribute.
Department	Enter the Directory attribute where the user's department information is stored. By default, in Active Directory, this is the department attribute.
Manager	Enter the Directory attribute where the user's manager information is stored. By default, in Active Directory, this is the manager attribute.

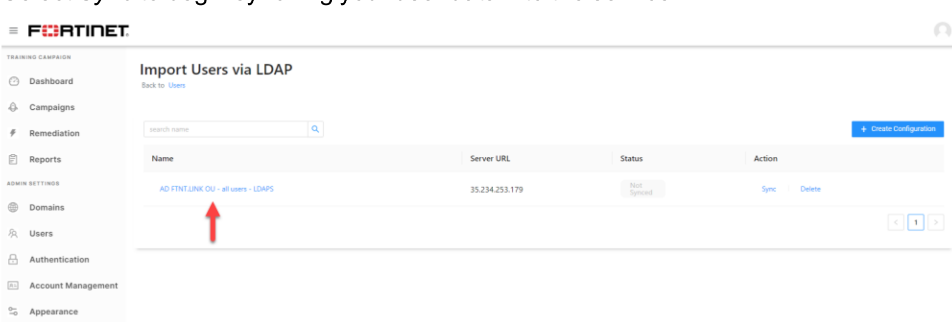
5. Click *Save the Configuration*.



The *Import User via LDAP* page is displayed with your configuration saved.



6. Select *Sync* to begin synching your user data into the service.

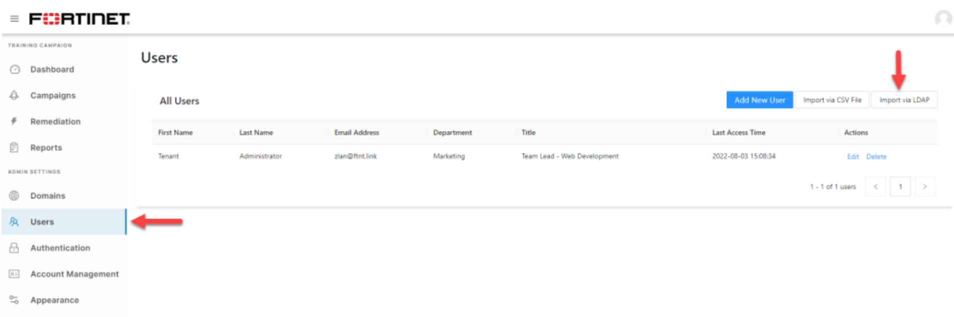


Modifying an Existing Configuration:

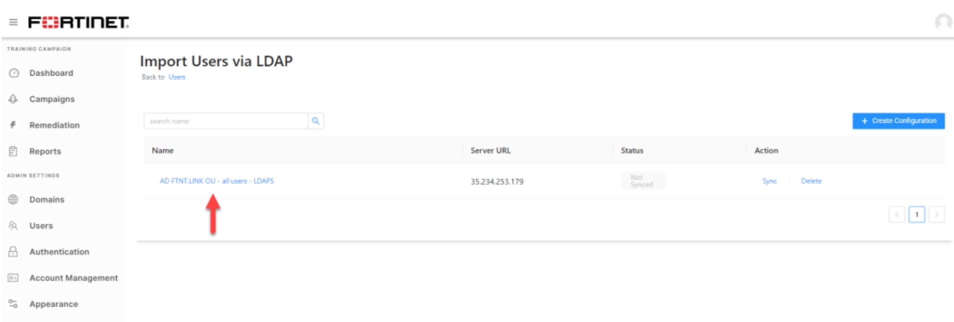
Should an existing *Import Users via LDAP* configuration require modification, you can modify the configuration.

To modify an existing configuration:

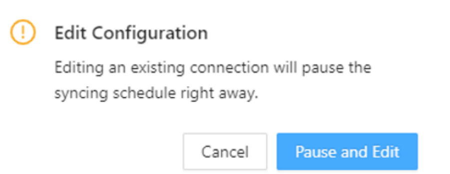
1. Go to *Users*, then select *Import via LDAP*.



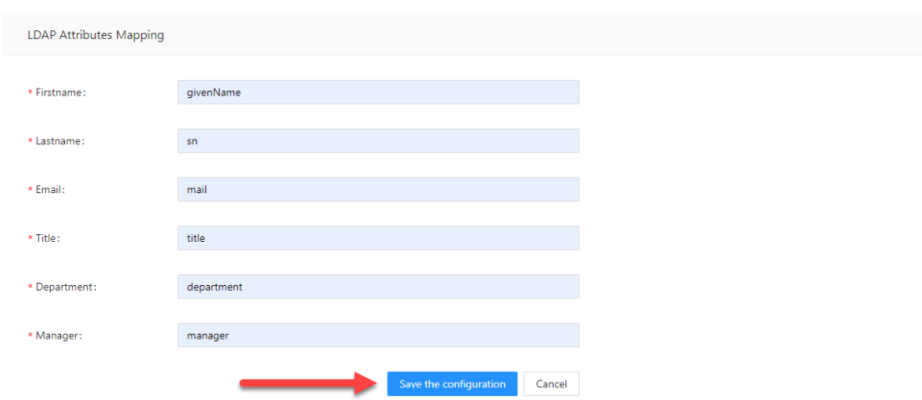
2. Click on the *Name* for the configuration you wish to modify.



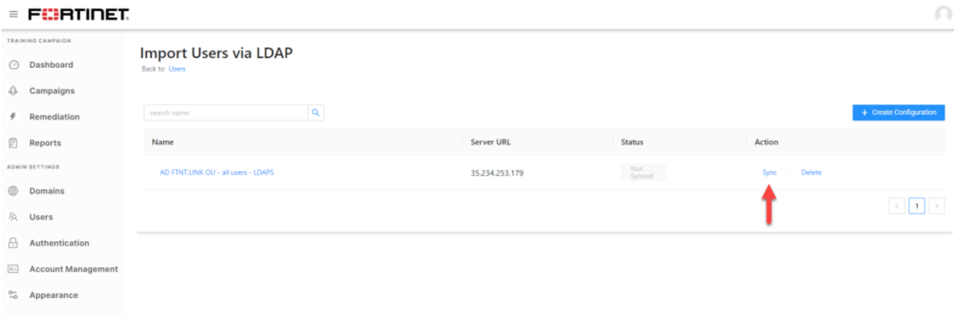
You will be prompted to *Pause and Edit* or *Cancel* the *Edit Configuration*.



3. Modify any information that you wish to change and select *Save the Configuration*.



4. Select *Sync*.



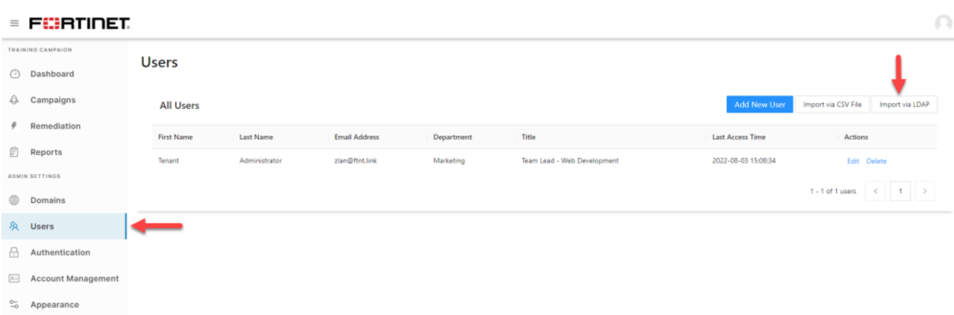
Deleting an Existing Configuration:

Deleting *Import Users via LDAP* configurations will:

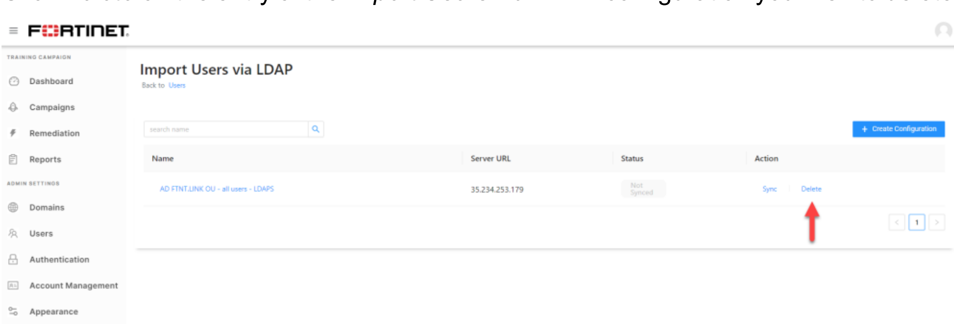
- Remove the configuration from the interface.
- Archive any users (including metadata, such as campaign and module information) that are part of this configuration. You will not be able to see user information or assign these users to Campaigns in the service. If the user is re-added as part of a new configuration, their user meta data will return.
- Return your Allocated user count to the number in use minus the count of users contained within the deleted LDAP configuration.

To delete an Import Users via LDAP configuration:

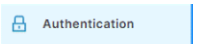
1. Go to *Users*, then select *Import via LDAP*.



2. Click *Delete* on the entry of the *Import Users via LDAP* configuration you wish to delete.



Authentication - Configuring SAML2 single sign on

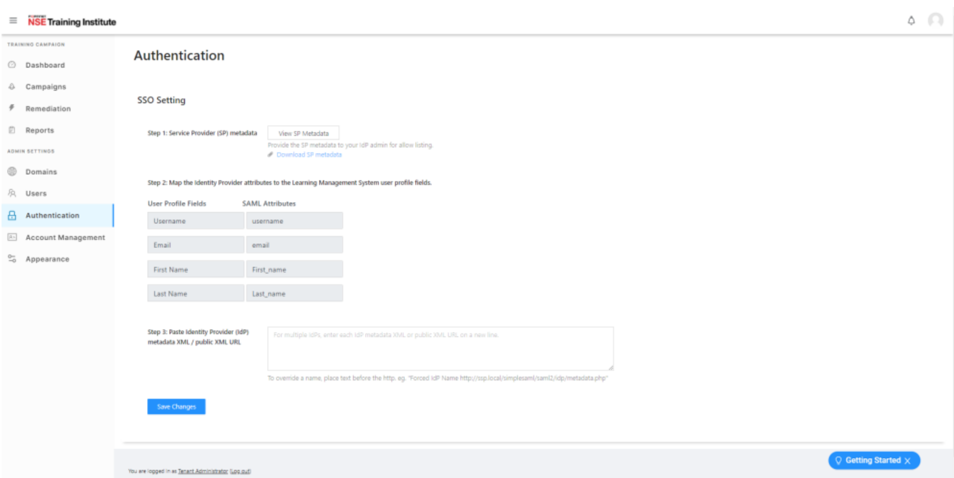


You must complete the domain configuration and validation steps before completing this configuration.

Once you have configured your Single Sign On (SSO) solution, students must use single sign on in order to log into the Learning Application.

Users must have a configured account in your Single Sign On solution in order to access the Learning Application.

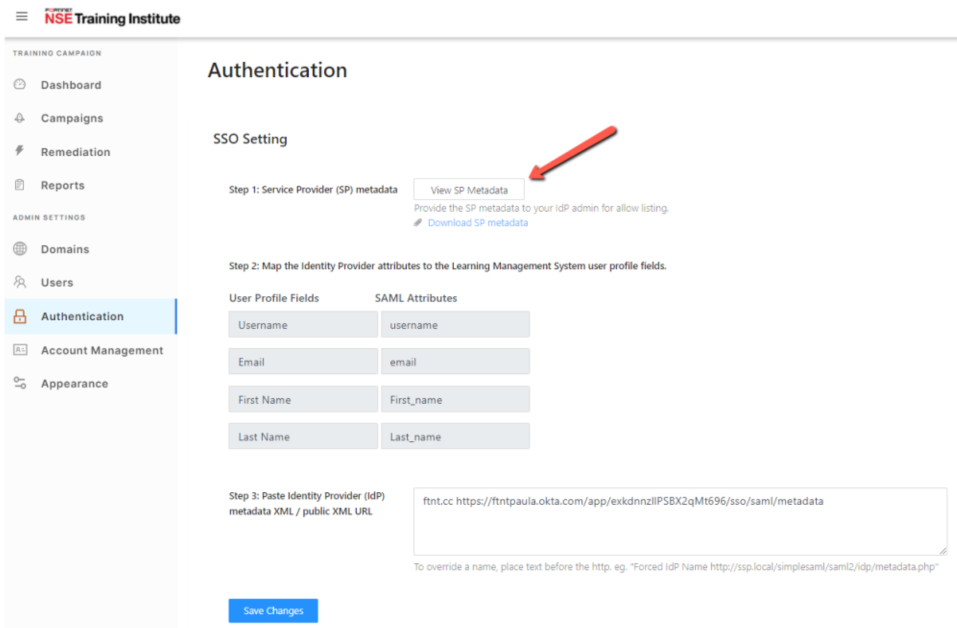
The Security Awareness and Training Service allows Customers and Partners to share metadata to establish a baseline of trust and interoperability using the XML based Security Assertion Markup Language (SAML) standard.



To configure SSO:

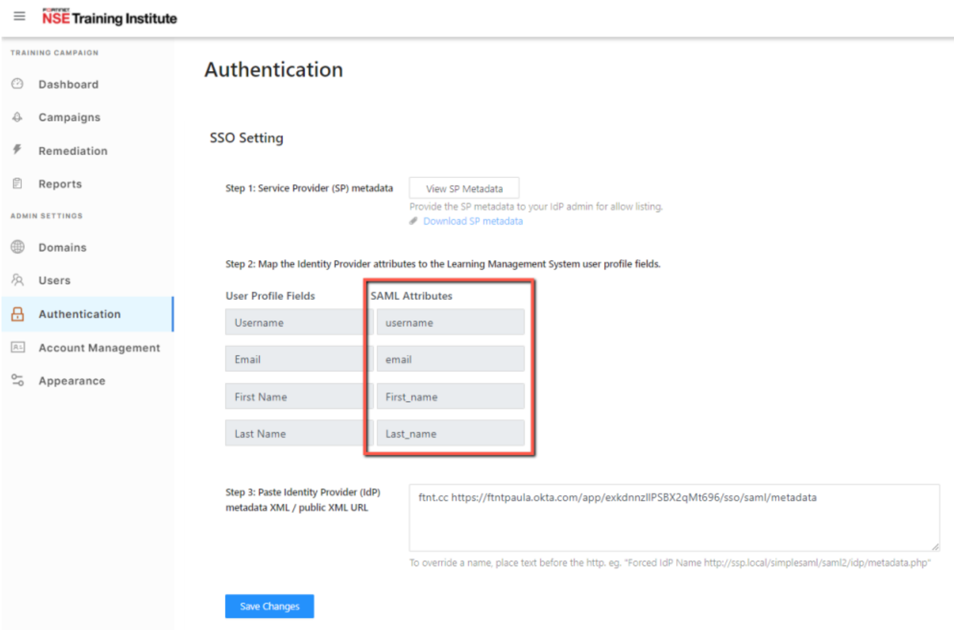
1. Download and provide the SP (Service Provider) metadata to your IdP (Identity Provider).

   You can either view and copy, or download the SP data from the tenant. You can also provide the entityID to the Identity Provider. To view the SP metadata, click on *View SP Metadata*.



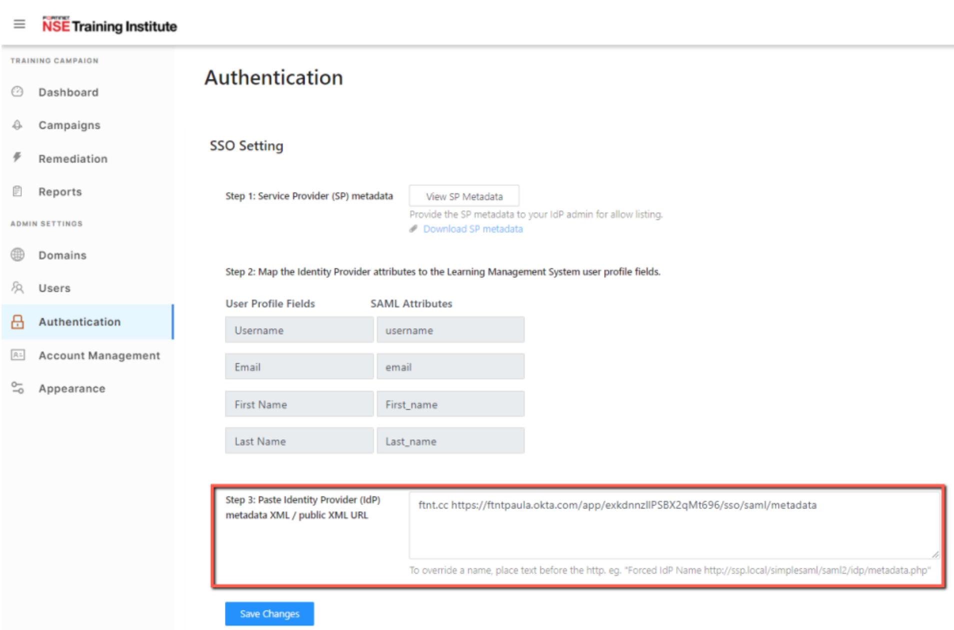
The metadata entityID link is highlighted in the following example:

2. The Identity Provider vendor must map the Identity Provider *SAML Attributes* to the Admin Portal *User Profile Fields* (which the tenant displays). The IdP provider will have fields in their system that must map to the *SAML Attributes* (they will need to use the exact attributes and case in the *SAML Attributes* highlighted below).

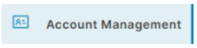


Assume case sensitivity when mapping the SAML Attributes.

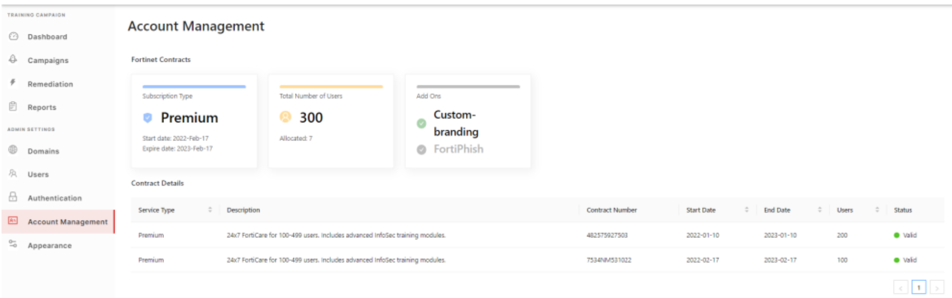
3. Paste the Identity Provider (IdP) metadata XML/public XML URL information into the *Identity Provider (IdP) metadata XML / public XML URL* field and select *Save Changes.*



Account management



Custom branding licenses do not show up in the list, currently. You will see the contract present in the *Fortinet Contracts* section.



There are three main sections to *Account Management*.

Fortinet Contracts

This section provides the Customer or Partner with:

- *Subscription Type* (Free, Standard, or Premium): This section dictates which services are included with their purchase. It also includes information on the start and end dates of the contract.
- *Total Number of Users*: This shows the total number of licenses purchased as well as how many licenses are currently in use.

Contract Details

This section includes an audit of the contracts that have been purchased by the customer. It includes the following information:

- *Service Type*: Free, Standard, or Premium.
- *Description*: Support information, number of users, and modules included.
- *Contract Number*: The number of the contract the service was purchased under.
- *Start Date*: The date the service was purchased and is active from.
- *End Date*: The date the service expires.
- *Users*: The number of licenses purchased.
- *Status*: The current status of each contract (Valid, Pending, or Expired)

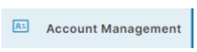
Customer Account Management

This section is available for Partners only.

This section includes information on each account and allows Administrators to Activate Service and Log in. It includes the following information:

- *Email of the Administrator*
- *Account Number*
- *Service Status*
  - *Pending*: An invitation has been sent to the customer to log in to the new tenant.
  - *Completed*: The customer has received the invitation and logged in to the new tenant.
- *Action* (Log in)

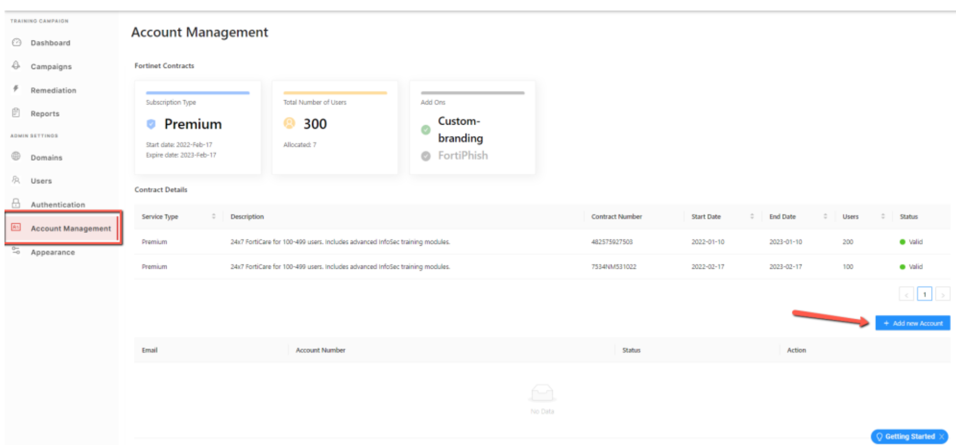
Adding a customer account (Partners only)



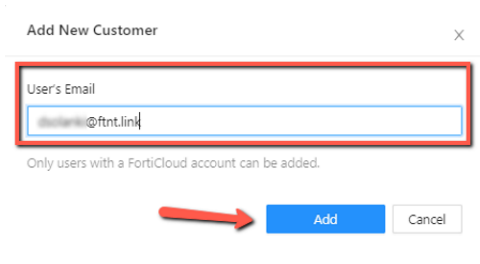
Partners can configure access to their customer's tenants so that they can log in from their own Partner tenant in order to manage their customer's tenants. This requires the Customer grant access to the Partner for these purposes.

To add a customer account:

1. Go to *Account Management*. In the bottom half of the screen, select *Add new Account*.



2. In the *Add New Customer* dialog, enter the email for the customer's FortiCare Support account and select *Add*.

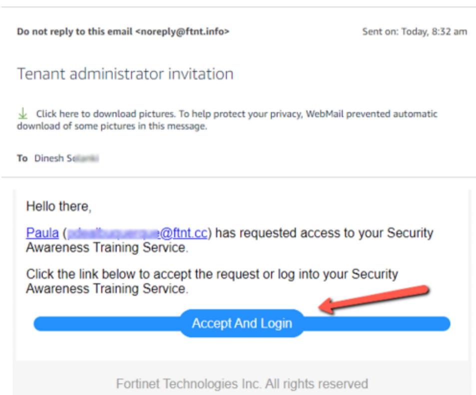


You will see an entry for the Customer which includes details for the request:

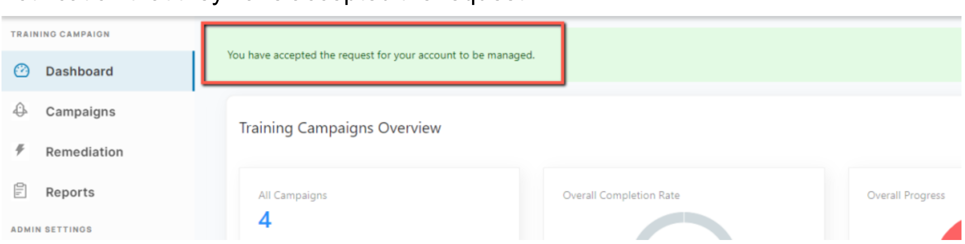
- Email
- Account Number
- Status (Pending until the customer accepts the invite that was sent to them).
- The *Action / Log In* button (grayed out until the customer accepts the invite).

Customers can also delete these entries should the Partner relationship change.

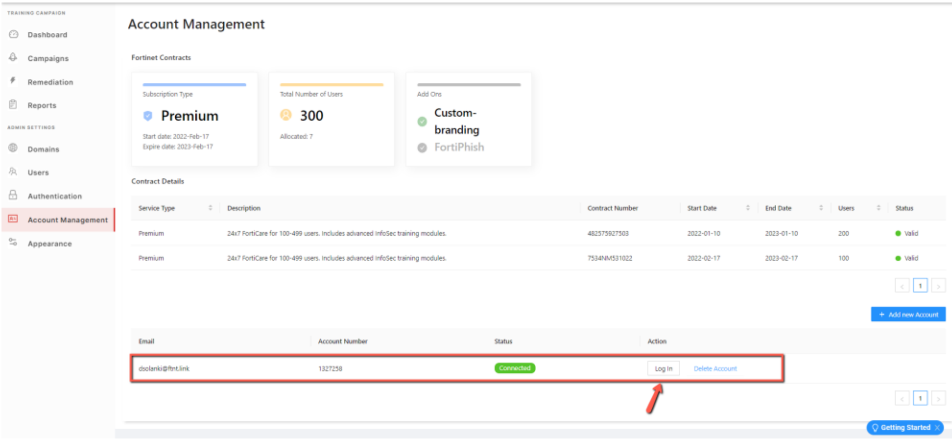
3. The Customer will receive an email with the invitation where they can choose to *Accept and Login*.



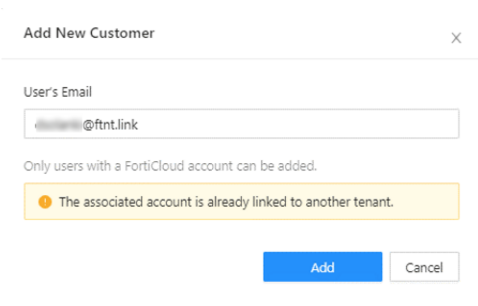
4. The Customer then logs in to the account when prompted. Once successfully logged in, they will receive a notification that they have accepted the request.



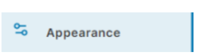
5. The Partner will now also be able to log in to the Customer tenant from the Account Management page.



Customers can only provide access to a single Partner account. If an attempt to add a second account occurs, an error will be presented: *The associated account is already linked to another tenant*.

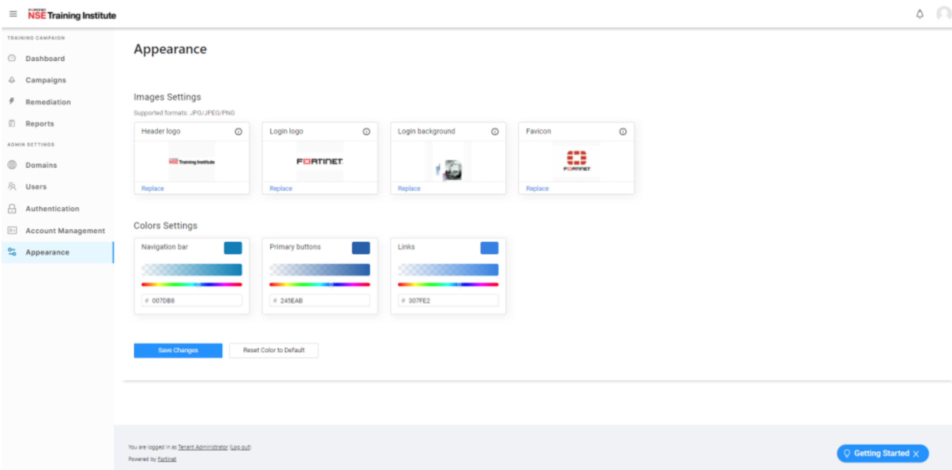


Appearance (Premium service only)



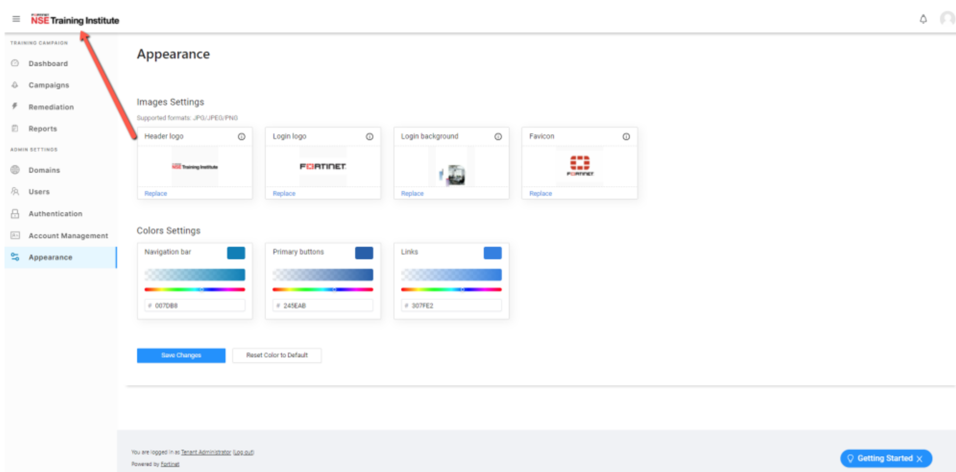
Depending on the licensing purchased, Customers and Partners can customize the branding and colors of their Admin Portal Tenant from the *Appearance* page.

This feature is only available for Premium licenses (Free 25 user Premium, which if for Partners only, and Premium, which is purchased by the Customer) it is not available for free and Standard license codes.

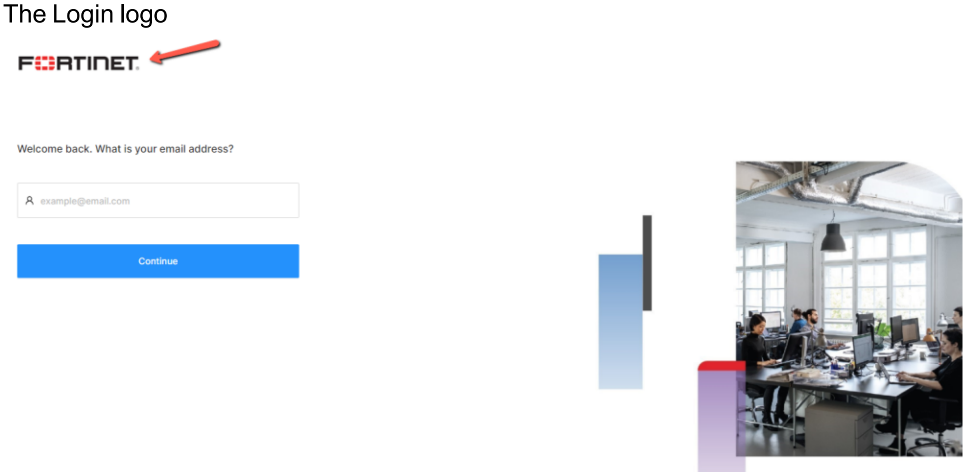


You can modify images and colors by selecting to upload or replace image files, or change the color codes for specific items per below:

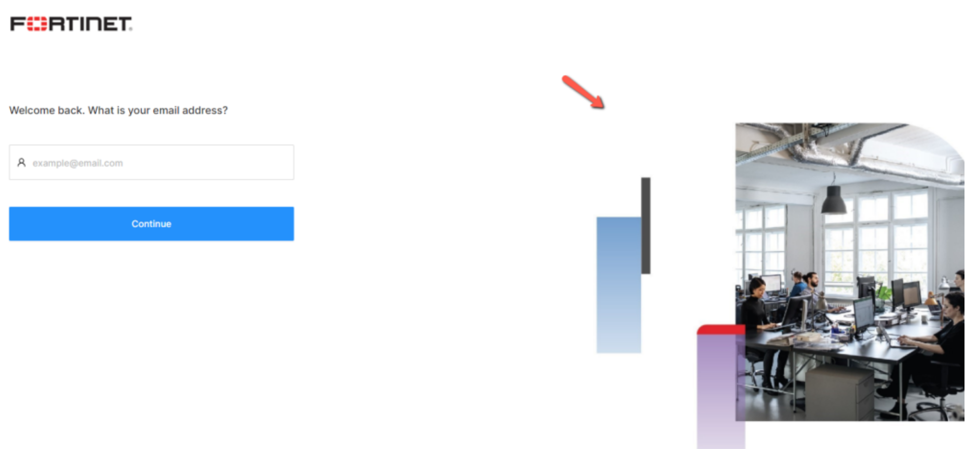
- The Header logo



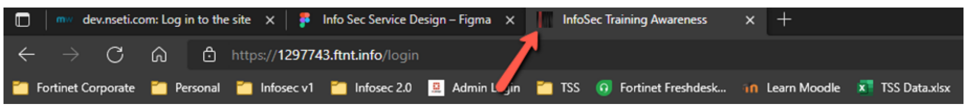
- The Login logo



- The Login background image

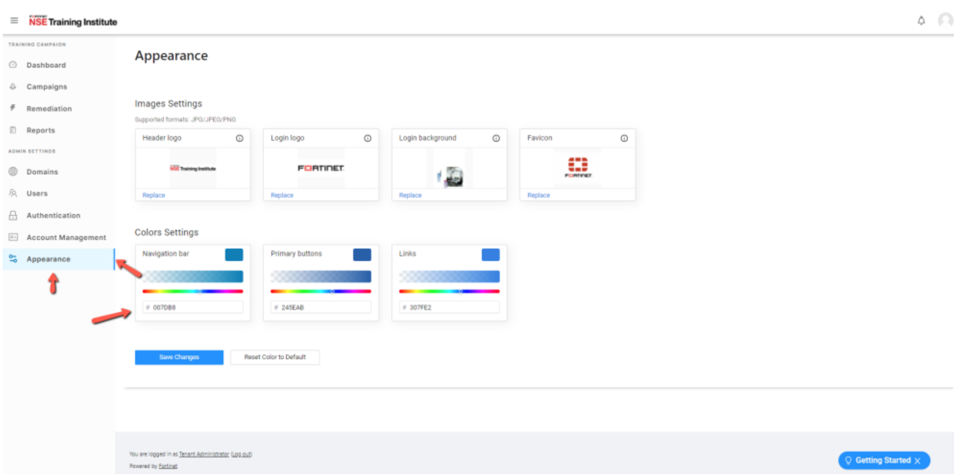


- The Favorite icon (Favicon) image

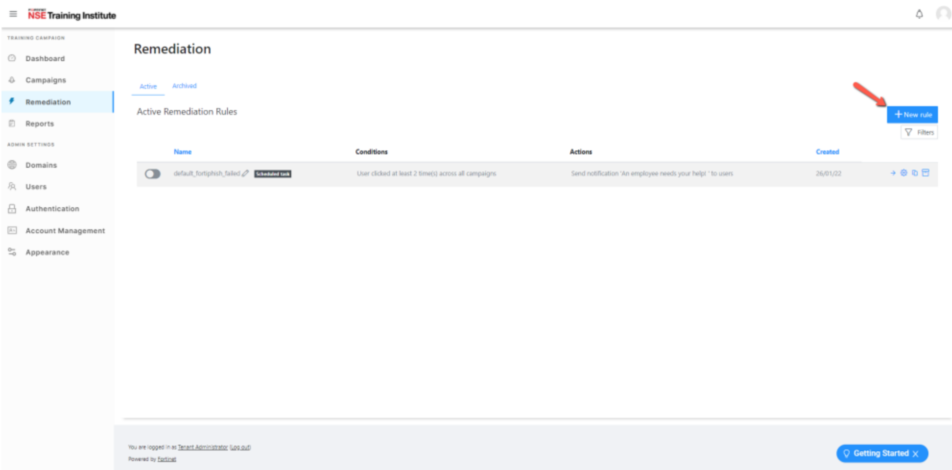


You can also upload your branding colors to change the appearance on your Tenantss by modifying the following:

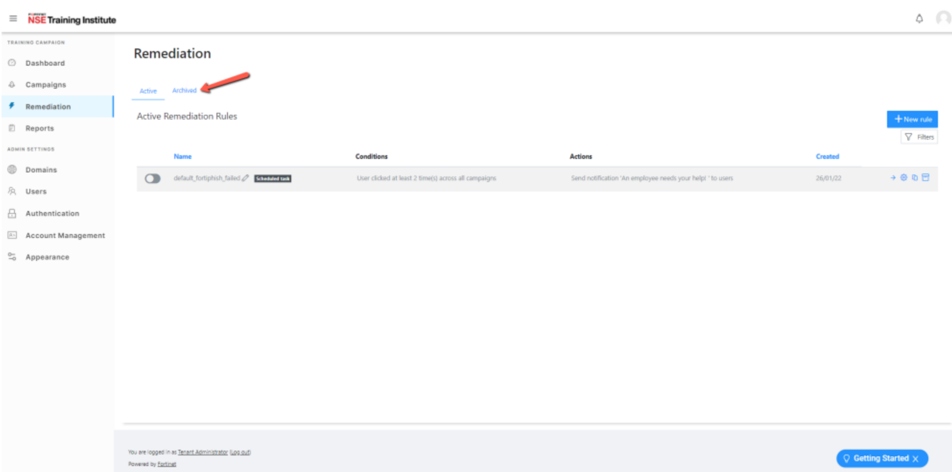
- The Navigation bar color



- The primary buttons color



- The links color



Custom-brand (Add-on)

This feature is only available for Premium licenses (Free 25 user Premium and Premium). It is not available for free and Standard license codes.

This component requires the purchase of an additional license string.

- When a customer who does not have an MSSP Partner relationship purchases the Custom-brand add on, the header logo configured on the *Appearance* page will display in both the upper left and lower right-hand corners of the Learning Application. If not purchased, the customer will see the Fortinet logo in the lower right-hand corner of the Learning Application.
- When Custom-brand add-on is purchased by a Partner, the Partner header logo will appear in the bottom right corner of the Customer's Learning Application screens. This matches the header logo setting configured in the Partner tenant *Appearance* page settings.

If you have purchased custom branding, please contact Security Awareness and Training Service Support by sending an email to infosec_awareness@fortinet.com.

Do not reply on previous case email threads. Please send a new email thread.

Assets

The *Assets* available to customers depend on the level of service purchased or whether the tenant administrator has been granted partner level permissions.

Awareness Assets

Create a culture of cybersecurity awareness within your company by downloading and deploying these customizable assets.

The first time you access the *Assets*, you will need to select the *Enroll* button.

Co-branded Assets

These assets are available with Premium subscription level and to Partner organizations.

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

- Banners
- Emails
- Posters
- Screen Savers
- Tip Sheets
- Videos - no logos

Custom Branding

These assets are available with purchase of the Custom-brand Add-on only.

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

- Banner
- Email
- Posters

- Screen Savers
- Tip Sheets
- Videos

Fortinet Assets

These assets are available with Standard or Premium subscription level and to Partner organizations.

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

- Banners
- Emails
- Posters
- Screen Savers
- Tip Sheets
- Videos

K-12 School Assets

These assets are available with Premium subscription level and to Partner organizations.

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

- K12 Email and reminder
- Banners
- Posters
- Screen Savers
- Tips Sheets

Nano Videos

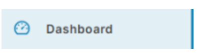
Typically less than one minute, nano modules can be used to reinforce a topic or as aids and assets to promote security awareness throughout an organization.

- Generic Videos
- K-12 Videos

Training campaigns

This section contains the following topics:

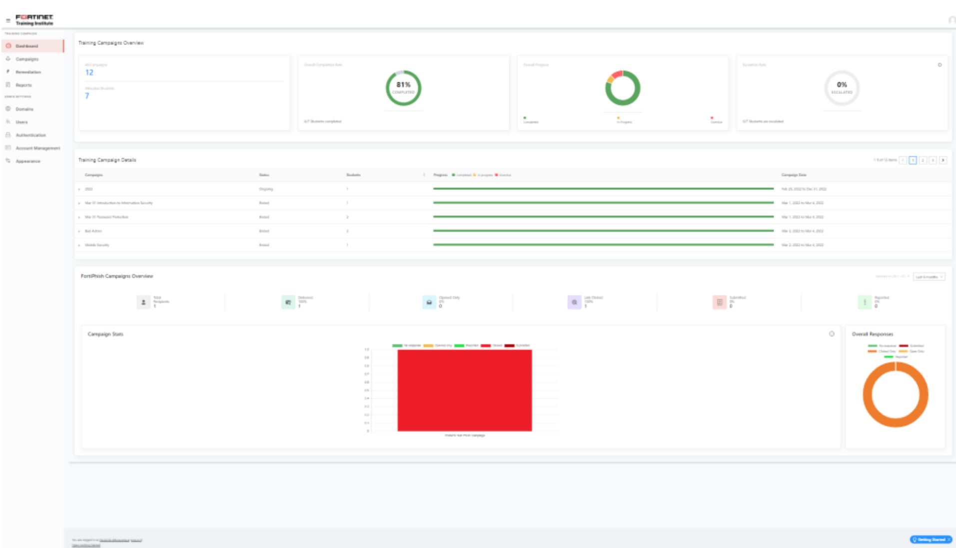
Dashboard



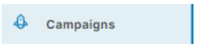
The *Dashboard* page appears when you log in to the tenant as the main and default screen. You can also access the dashboard at any time by selecting the *Dashboard* icon in the Navigation Menu.

The *Dashboard* shows information such as:

- *Training Campaign Overview*
- *Training Campaign Details*
- *FortiPhish Campaigns Overview* (if configured)



Campaigns



Campaigns allow Administrators to establish the learning content which will then be assigned to learners. Administrators can choose some, or all modules, from the following lists.

Modules and videos included with the Standard level of service

Generic modules	K-12 modules
Introduction to Information Security	Introduction to Information Security for Educators
Bad Actors	Bad Actors for Educators
Social Engineering	Social Engineering for Educators
Phishing Attacks	Phishing Attacks for Educators
Email Security	Email Security for Educators
Malware and Ransomware	Malware and Ransomware for Educators
Password Protection	Password Protection for Educators

Micro modules (Generic)	Micro modules (K-12)
Social Engineering	Social Engineering for Educators
Phishing Attacks	Phishing Attacks for Educators
Email Security	Email Security for Educators
Malware and Ransomware	Malware and Ransomware for Educators
Password Protection	Password Protection for Educators

Nano videos (Generic)	Nano videos (K-12)
Shoulder Surfing	Shoulder Surfing for Educators
Tailgaiting	Tailgaiting for Educators
See Something, Say Something	See Something, Say Something for Educators
Follow Company Policy	Follow Company Policy for Educators
Avoid Unknown Wi-Fi Networks	Avoid Unknown Wi-Fi Networks for Educators
Good Password Hygiene	Good Password Hygiene for Educators
Think Before You Click	Think Before You Click for Educators

Modules and videos included with the Premium level of service

Generic modules	K-12 modules
Introduction to Information Security	Introduction to Information Security for Educators
Bad Actors	Bad Actors for Educators
Social Engineering	Social Engineering for Educators
Phishing Attacks	Phishing Attacks for Educators
Email Security	Email Security for Educators
Malware and Ransomware	Malware and Ransomware for Educators
Password Protection	Password Protection for Educators
Multi-Factor Authentication	Multi-Factor Authentication for Educators
Data Security	Data Security for Educators
Data Privacy	Data Privacy for Educators
Access Control	Access Control for Educators
Mobile Security	Mobile Security for Educators
Insider Threat	Insider Threat for Educators
Clean Desk Policy	Clean Desk Policy for Educators
Working Remotely	Working Remotely for Educators
Web Conference Security	Web Conference Security for Educators
Business Email Compromise	Business Email Compromise for Educators
Intellectual Property	Intellectual Property for Educators
Secure Travel Tips	Secure Travel Tips for Educators
Social Media	Social Media for Educators

Micro modules (Generic)	Micro modules (K-12)
Social Engineering	Social Engineering for Educators
Phishing Attacks	Phishing Attacks for Educators
Email Security	Email Security for Educators
Malware and Ransomware	Malware and Ransomware for Educators
Password Protection	Password Protection for Educators
Data Security	Data Security for Educators
Data Privacy	Data Privacy for Educators
Business Email Compromise	Business Email Compromise for Educators

Micro modules (Generic)	Micro modules (K-12)
Insider Threat	Insider Threat for Educators
Clean Desk Policy	Clean Desk Policy for Educators

Nano videos (Generic)	Nano videos (K-12)
Shoulder Surfing	Shoulder Surfing for Educators
Tailgaiting	Tailgaiting for Educators
See Something, Say Something	See Something, Say Something for Educators
Follow Company Policy	Follow Company Policy for Educators
Avoid Unknown Wi-Fi Networks	Avoid Unknown Wi-Fi Networks for Educators
Good Password Hygiene	Good Password Hygiene for Educators
Think Before You Click	Think Before You Click for Educators
Web Conference Tips	Web Conference Tips for Educators
Travel Tips	Travel Tips for Educators
Back Up Your Data	Back Up Your Data for Educators
Good Mobile Habits	Good Mobile Habits for Educators
Encrypt Sensitive Data	Encrypt Sensitive Data for Educators
Update Your Software	Update Your Software for Educators
Protect Your Devices	Protect Your Devices for Educators
Non-discoverable Bluetooth	Non-discoverable Bluetooth for Educators
Use Multi-factor Authentication	Use Multi-factor Authentication for Educators
Device Disposal	Device Disposal for Educators
Enable Screen Locks	Enable Screen Locks for Educators
Clean Desk Tips	Clean Desk Tips for Educators
Phishing Attacks	Phishing Attacks for Educators

Campaign templates included with the Premium level of service

For Premium profile customers, in addition to the Premium profile modules listed above, the system comes pre-loaded with several, generic Campaign Templates. These contain the following content and modules:

- Manager Modules
  - Security Awareness for Managers
  - Cyber Security Frameworks for Managers
  - Deploying and Managing the Fortinet Security Awareness and Training Service
- Common Attacks

    - Social Engineering
    - Phishing
    - Business Email Compromise
- Authentication
    - Password Protection
    - Multi-Factor Authentication
    - Access Control
- Data Privacy and Security
    - Mobile Security
    - Data Security
    - Email Security
    - Data Privacy
    - Intellectual Property
- Physical Security
    - Insider Threat
- Online Safety
    - Working Remotely
    - Web Conference Security
    - Bad Actors
    - Social Media

For Premium profile customers, in addition to the Premium Profile modules listed above, the system comes pre-loaded with several, K-12 Campaign Templates for the Education Industry. These contain the following content/modules:

- Educators – Protecting Sensitive Data
    - Education – Bad Actors
    - Education – Clean Desk
    - Education – Data Privacy
    - Education – Data Security
    - Education – Insider Threat
    - Education – Introduction to Information Security
- Educators – Online and Email Best Practices
    - Education – Business Email Compromise
    - Education – Email Security
    - Education – Introduction to Information Security
    - Education – Phishing
    - Education – Social Engineering
    - Education – Social Media
    - Education – Web Conference Security
- Educators – Securing Your Digital World
    - Education – Bad Actors
    - Education – Insider Threat
    - Education – Introduction to Information Security
    - Education – Malware

- Education – Mobile Security
- Education – Multi-Factor Authentication
- Education – Password Protection

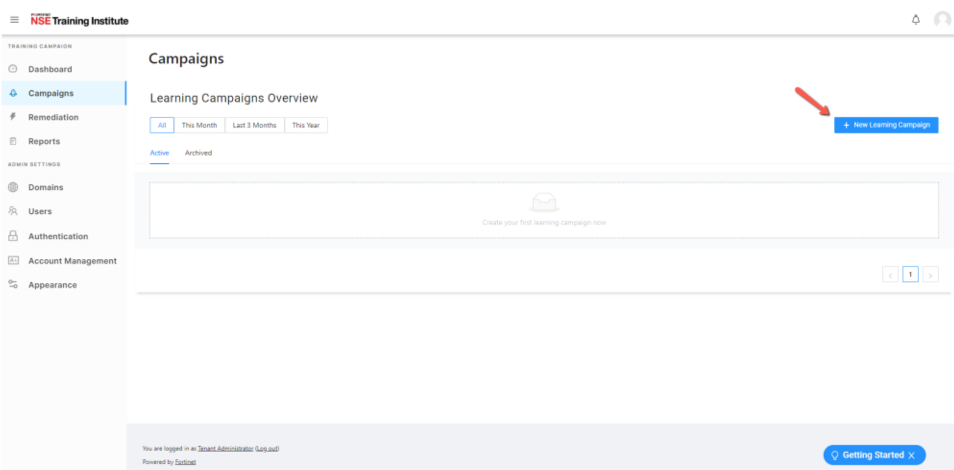
Campaign structure setup

Campaign Structure Setup allows Administrators to create or re-use Programs, setup start and end dates for the Campaign, and assign training to users. You can also archive Campaigns should they not be required any longer when you may want to re-introduce them later. Once a Campaign has been archived, it may also be deleted if no longer required.

Creating a new campaign from an existing template

To create a new campaign from an existing template:

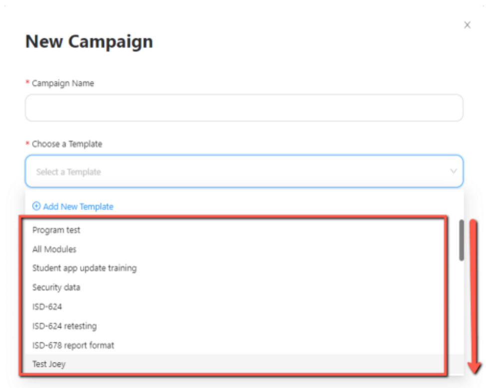
1. Go to *Campaigns*, then select *New Learning Campaign*.



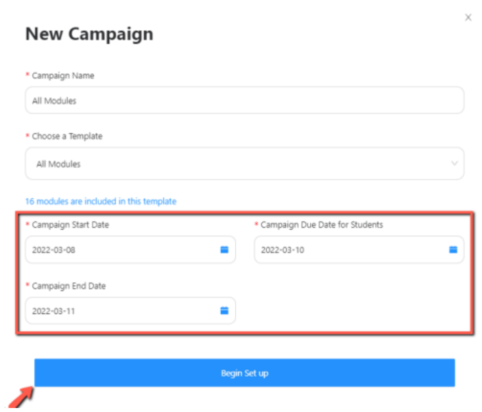
2. Give the new Campaign a meaningful name.

> For clarity, it is recommended you include a descriptive name and possibly a data stamp (month and year or quarter and year) in the name as well as a high-level description of the content or purpose.
>
> You can use a name of up to 256 characters.

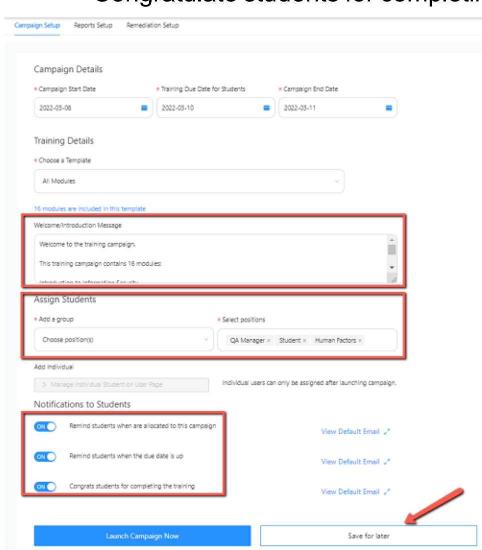
3. Choose a Template from the drop down list of existing entries below *Add New Template*.



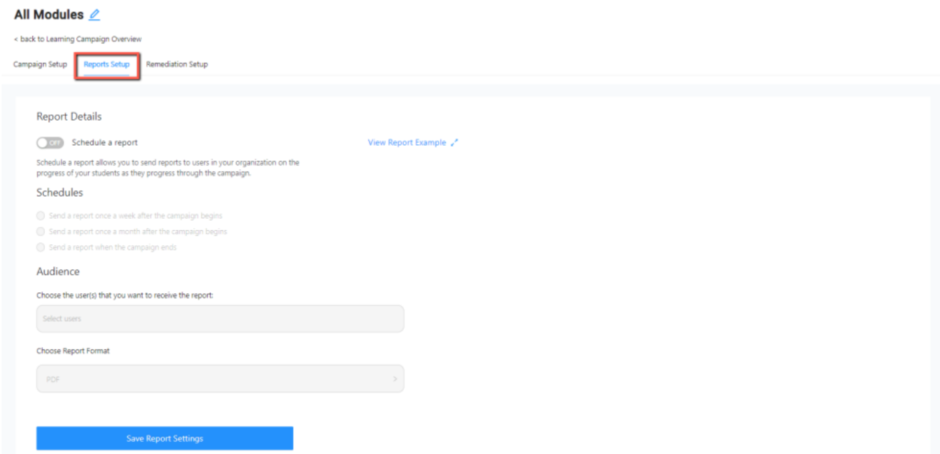
4. Enter a *Start Date*, *Due Date*, and *End Date* for the campaign and click *Begin Set up*.



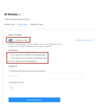
5. Complete the remaining fields in the *Campaign Details* page and select *Save for later*.
   - Enter a *Welcome/Introduction Message* that will be presented to the users.
   - *Add a group*: Assign users by Department or Position.
   - Choose which *Notifications* students should receive:
     - Remind students when they are allocated to this campaign
     - Remind students when the due date is up
     - Congratulate students for completing the training



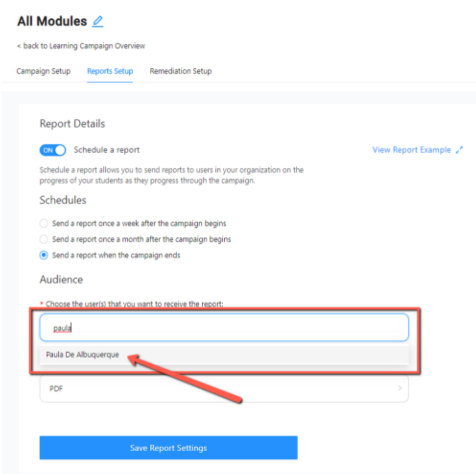
6. Select the *Reports Setup* tab.



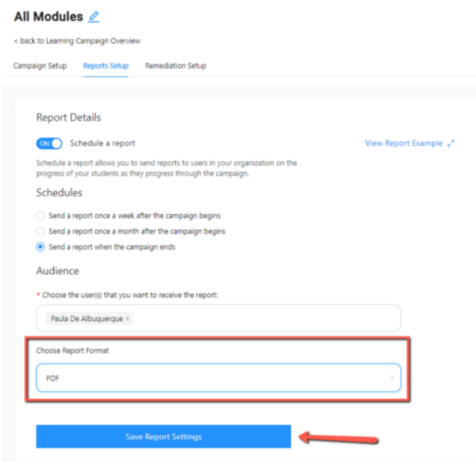
7. Turn on *Schedule a report* and select the *Schedule*.



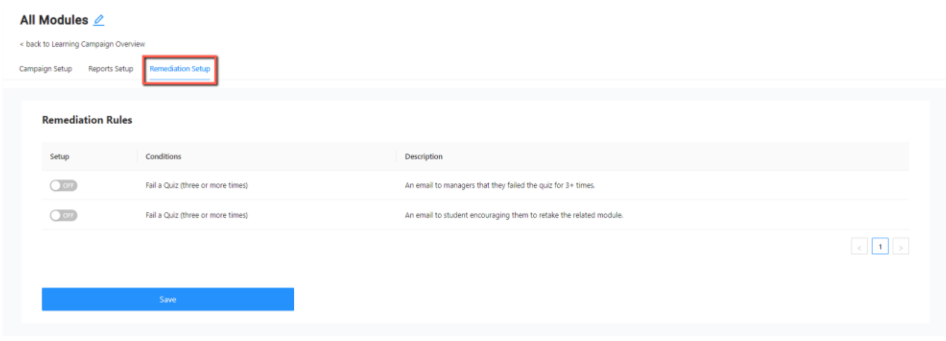
8. Choose the *Audience* for the report by typing the names of the people in the *Choose the user(s) that you want to receive the report* and selecting them.



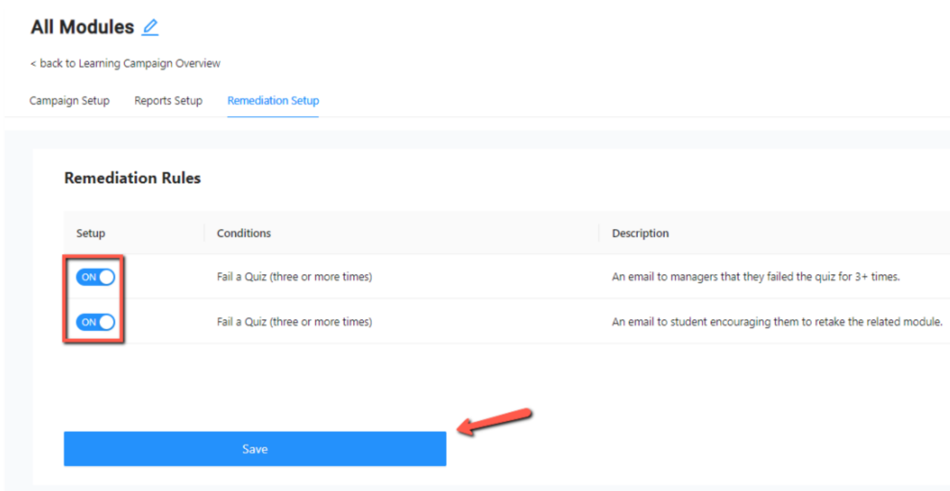
9. Select a report format (PDF, EXCEL, CSV) from the *Choose Report Format* drop down menu and then select *Save Report Settings*.



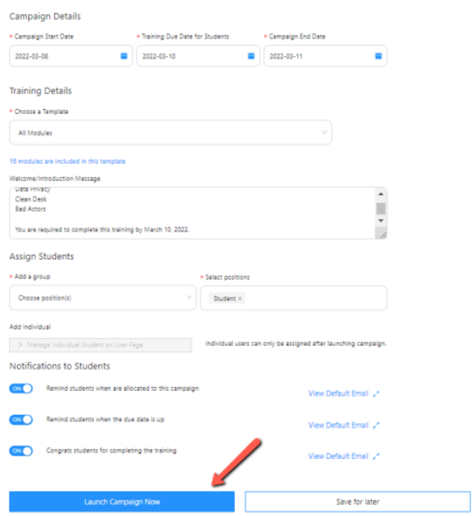
10. Click on *Remediation Setup* tab (this requires that you included the manager email field when you imported your users using a .csv file).



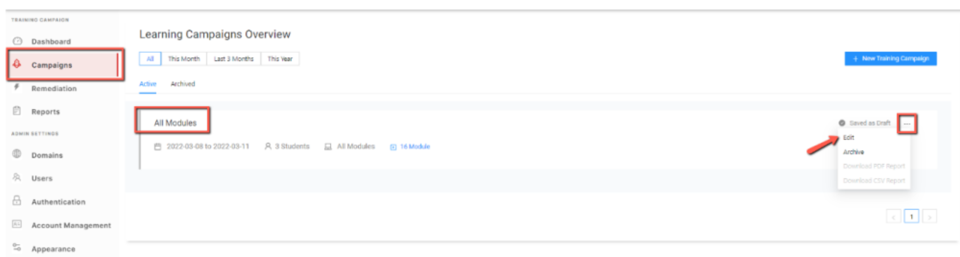
11. Turn off either or both of the switches to enable the *Remediation Rules* (email manager and email student) and click *Save*.



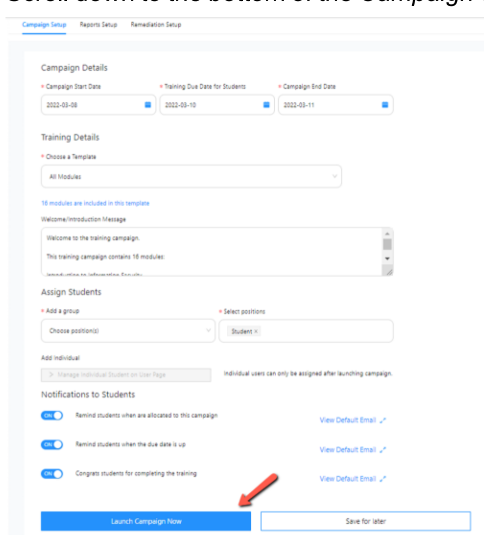
12. If you are ready to launch the campaign immediately:
    a. Return to the *Campaign Setup* tab.
    b. Select *Launch Campaign Now*.



13. If you wish to start the campaign at a later date:
    a. Select *Save for later*.
    b. Return to the *Campaigns* Navigation Menu.
    c. Locate the campaign.
    d. Select the … to the right of the screen.
    e. Select *Edit*.



    f. Scroll down to the bottom of the *Campaign Setup* page and select the *Launch Campaign Now* button.

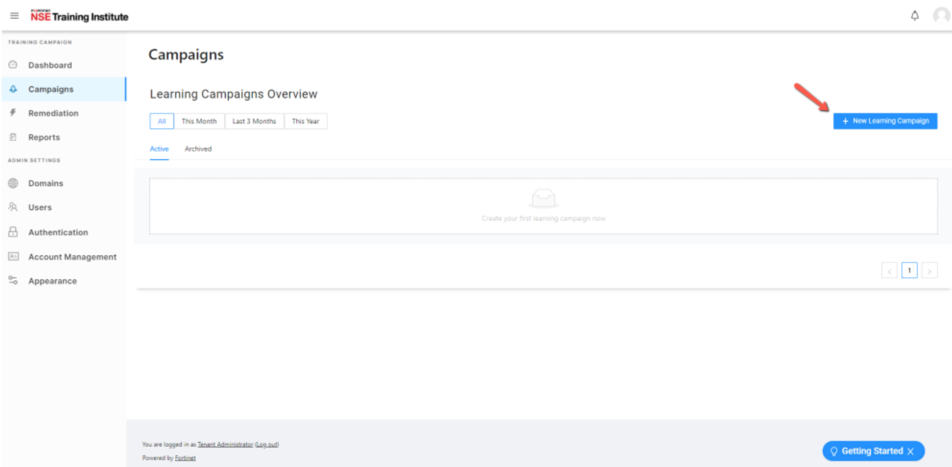


Creating a new template from the module list

You can create your own Template/Program choosing only the modules you wish to include.

To create a new template:

1. Go to *Campaigns*, then select *New Learning Campaign*.

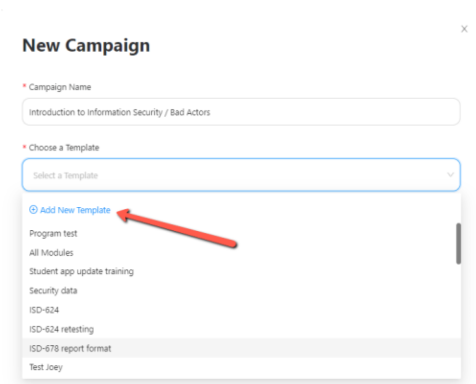


2. Give the new Campaign a meaningful name.

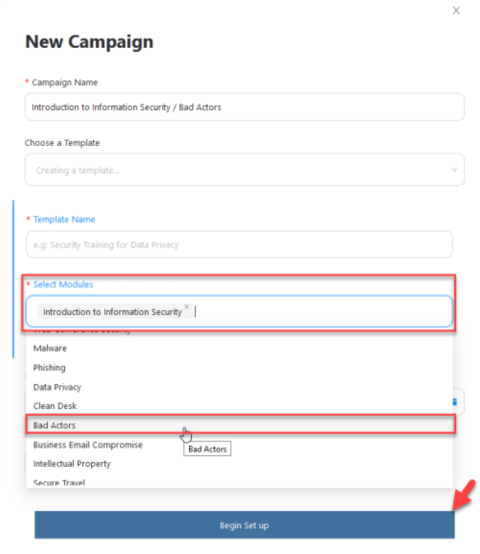
For clarity, it is recommended you include a descriptive name and possibly a data stamp (month and year or quarter and year) in the name as well as a high-level description of the content or purpose.

You can use a name of up to 256 characters.

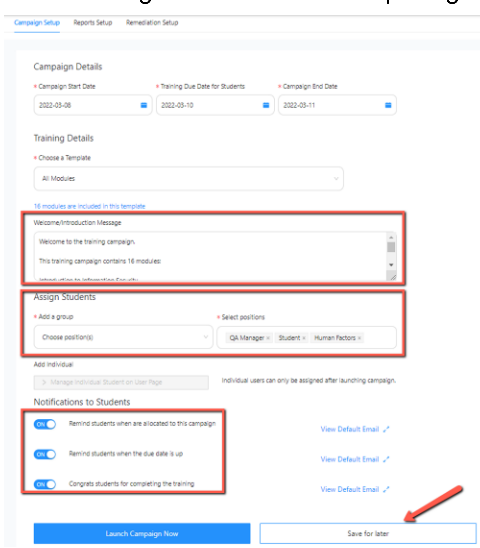
3. Click *Add New Template*. The + will change to a -.



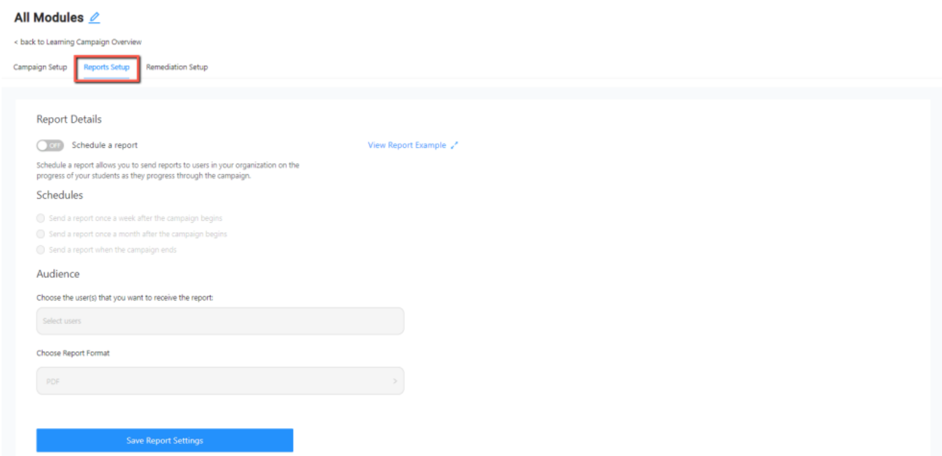
4. Click on the white background to hide the dropdown menu (or wait for it to disappear).
5. Click on each of the modules you wish to include in the new Template/Program.



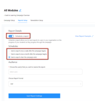
6. Complete the remaining fields in the *Campaign Details* page and select *Save for later*.
   - Enter a *Welcome/Introduction Message* that will be presented to the users.
   - *Add a group*: Assign users by Department or Position.
   - Choose which *Notifications* students should receive:
     - Remind students when are allocated to this campaign
     - Remind students when the due date is up
     - Congrats students for completing the training



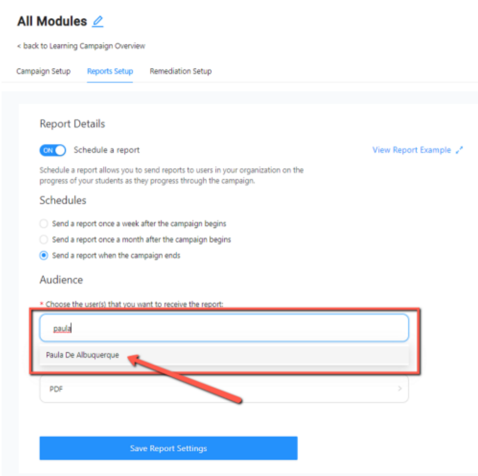
7. Select the *Reports Setup* tab.



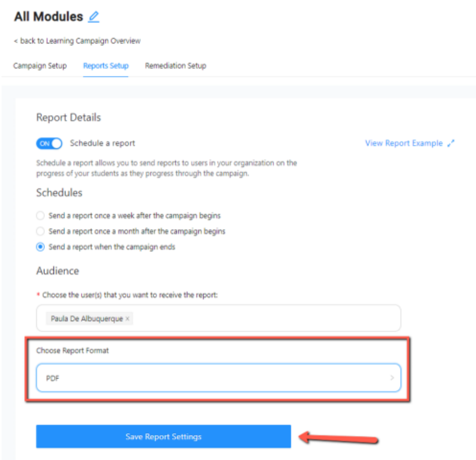
8. Turn on *Schedule a report* and select the *Schedule*.



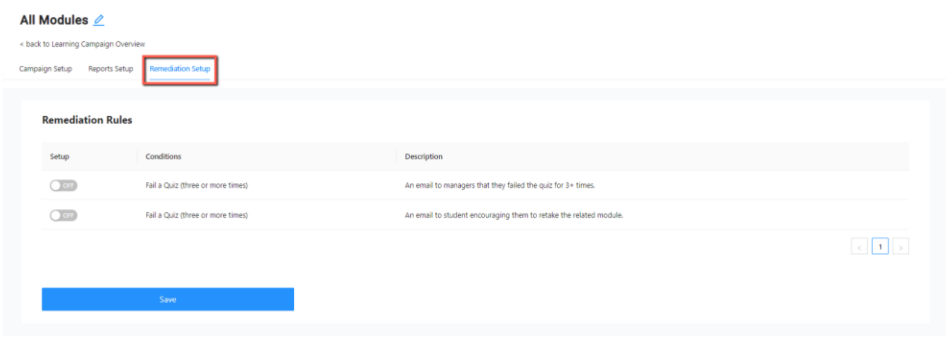
9. Choose the *Audience* for the report by typing the names of the people in the *Choose the user(s) that you want to receive the report* and selecting them.



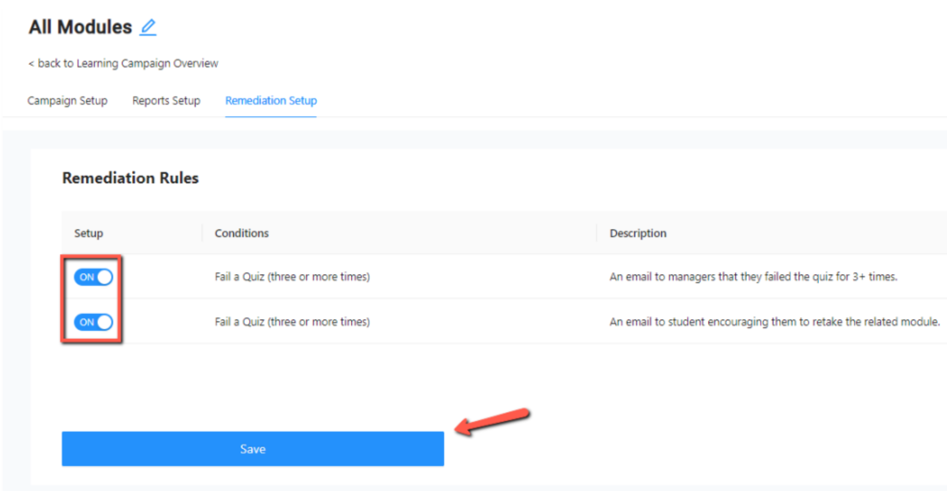
10. Select a report format (PDF, EXCEL, CSV) from the *Choose Report Format* drop down menu and then select *Save Report Settings*.



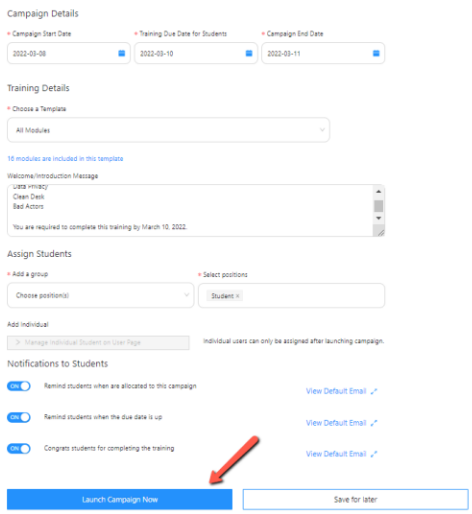
11. Click on the *Remediation Setup* tab (this requires that you included the manager email field when you imported your users using a .csv file).



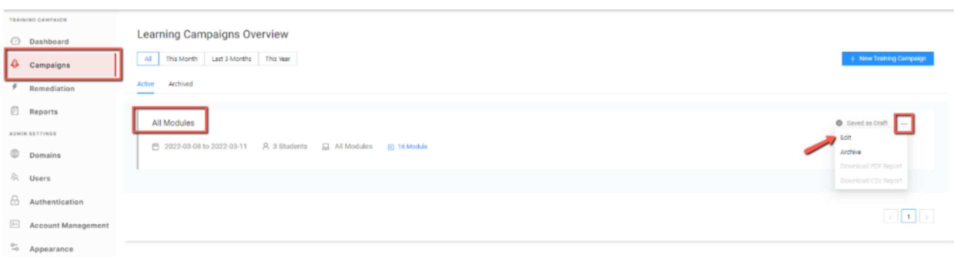
12. Turn off either or both of the switches to enable the *Remediation Rules* (email manager and email student) and click *Save*.



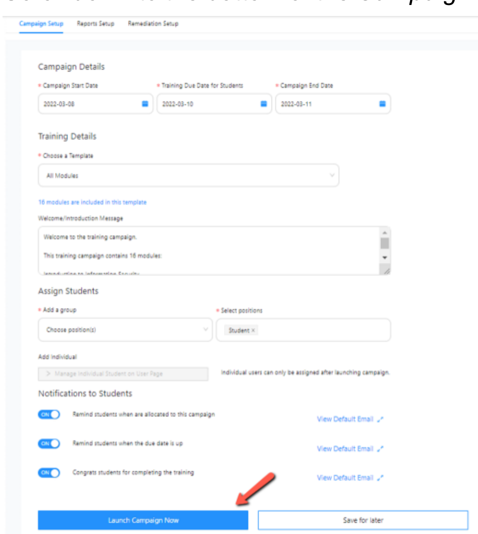
13. If you are ready to launch the campaign immediately:
    a. Return to the *Campaign Setup* tab.
    b. Select *Launch Campaign Now*.



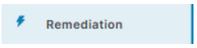
14. If you wish to start the campaign at a later date:
    a. Select *Save for later*.
    b. Return to the *Campaigns* Navigation Menu.
    c. Locate the campaign.
    d. Select the … to the right of the screen.
    e. Select *Edit*.



    f. Verify the *Campaign Start Date*, *Training Due Date for Students*, and *Campaign End Date* are accurate, otherwise, update them.
    g. Scroll down to the bottom of the *Campaign Setup* page and select *Launch Campaign Now*.



Remediation



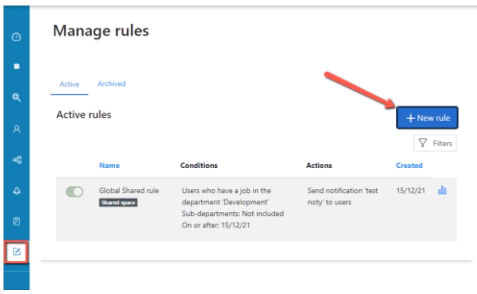
Selecting *Remediation* from the Navigation Menu gives you quick access to rules which affect your Campaigns.

Remediation allows you to do things like sending a notification to a student when they are allocated to a Campaign, issuing a certificate, badge, or a competence upon program completion, or sending a reminder when the program is overdue.

You can configure Conditions and applicable Actions (taken when the condition is met).

To set remediation actions:

1. Go to *Dynamic Rules*, then click *New rule.*

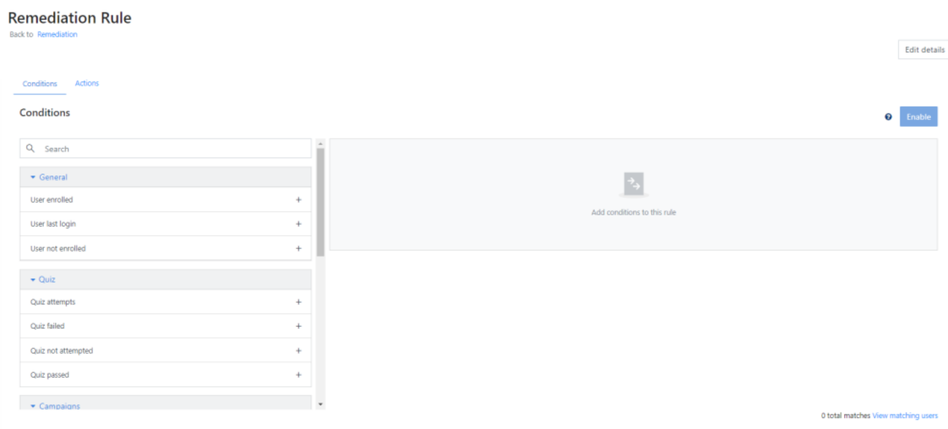


2. Give the Rule a meaningful name.
3. Select the *Rule action limits* checkbox.

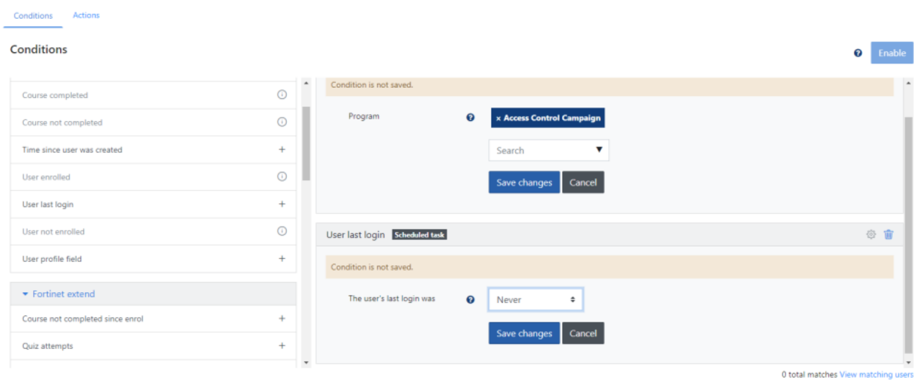
As soon as users match the rule conditions, the actions will be applied to them. These actions will not apply again if users continue to match the conditions. However, if a user stops matching and then matches again, the actions may be applied again. This setting defines the maximum number of times actions should apply.

---

4. Select *Save*. You are redirected to set your conditions.

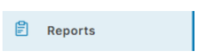


5. From the left-hand pane, select and configure each of the conditions you want the rule to match. There are several conditions (and associated sub conditions) you can match that fall under the following categories:
    - General
        - User enrolled
        - User last login
        - User not enrolled
    - Quiz
        - Quiz attempts
        - Quiz failed
        - Quiz not attempted
        - Quiz passed
    - Campaigns
        - Campaign certified
        - Campaign expired
        - Campaign not certified
        - Campaign overdue
        - Repeat campaign grace period ends
        - Repeat campaign period started
        - Users allocated to campaign
        - Users not allocated to campaign
    - Organization structure
        - User is in department
        - User is not in department
        - User has position
        - User doesn’t have position



6. Select *Save changes* for each *Condition* you have added.
7. Once you have configured your condition criteria, you can select the *Actions* tab to set what action should occur when the condition is met. Actions can also be configured for the following categories:
   - General
     - Notification
   - Campaigns
     - Allocate users to campaigns
     - De-allocate users from campaigns

Reports



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

- What type of information they would like to report on.
- What data should appear in the report (including any additional conditions, filters, and sorting they would like to apply).
- 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 in order to manage the user learning campaigns. Optionally, they can also create custom report data.

Standard, included reports, include:

- Advanced report
- FortiPhish

These reports require purchase of FortiPhish licensing.

- Campaigns

Selecting from standard reports setting up new (custom) reports

Custom reports can be set up in the *Reports* page.

To set up a report:

1. Select a report source:
    a. Select the fields you would like to include in the report from the *Table* tab.
    b. Assign any conditions.
    c. Assign filters.
    d. Select a sorting setting for the report data.
    e. Configure card view settings. The report will automatically switch to card view when displayed on small screens or in narrow blocks.
2. Choose the audience settings (Department and Positions) for who will receive a copy of this report.
3. Set the schedule for generation and distribution of the report.

Example of configuring a new custom report

The following is an example of configure a new custom report.

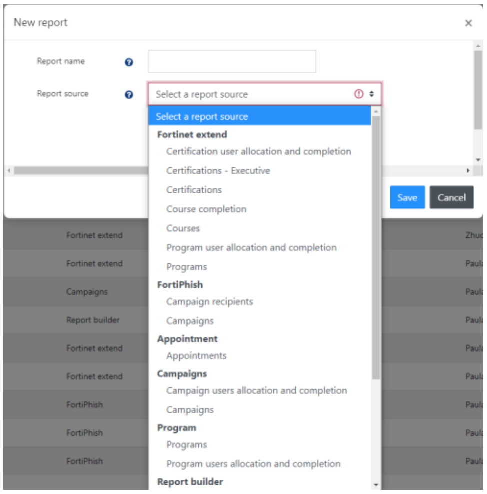
To configure a new custom report:

1. Go to *Reports*.
2. Select *New report*.
3. Give your report a name. This name should be meaningful and describe the purpose of the report.
4. From the *Report source* drop down menu, you can select from the following options:

Report categories	Report source						
Advanced report	Certification user allocation and completion	Certifications / Executive	Certifications	Course completion	Courses	Program user allocation and completion	Programs
FortiPhish	Campaign recipients	Campaigns					
Campaigns	Campaign users allocation and completion	Campaigns					

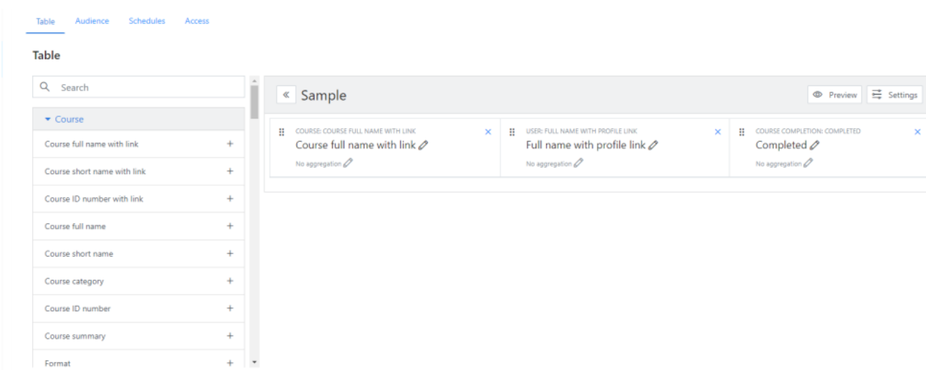
5. (Optional) Select the *Add default configuration* check box.

Each report source also defines default columns. If you want to create the report using the defaults, select this field. If you check this box, you can delete columns from the default list should you choose. You cannot re-add columns from default reports after you delete them. You must delete the report and start again.

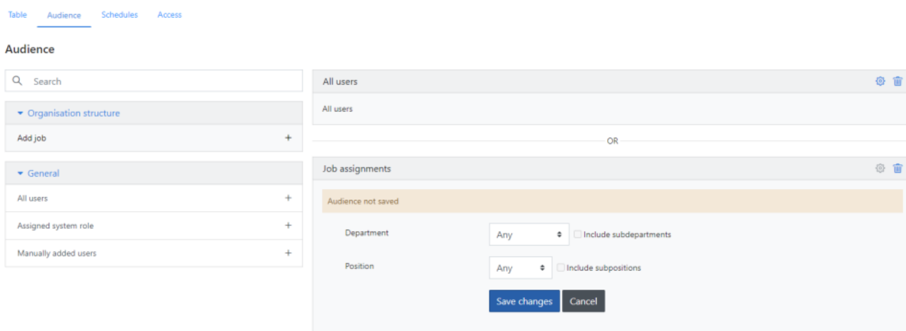


Once you select your data source and save the report, you can further customize the report:

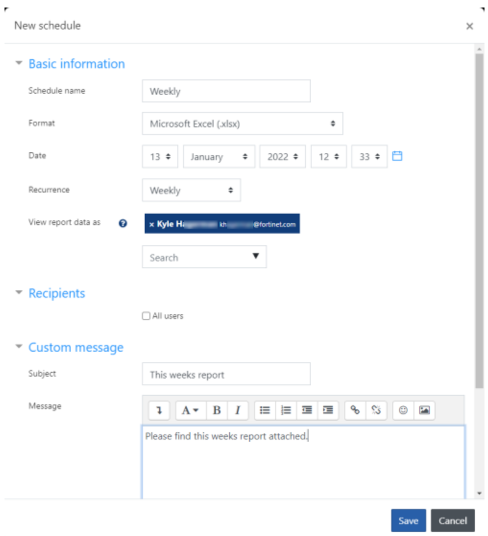
- *Table* data: What fields (columns) will be part of this report. The content of the report fields will depend on what source you selected in the first step.
- On the right hand side of the columns you have selected, you can select *Settings* to alternately configure:
  - *Conditions*: You can select from the field list above and then select modifiers (such as contains, doesn't contain, is equal to, and so on).
  - *Filter*: You can select from the field list above and then select Filters (a list of filters that do not immediately apply but are available to users)
  - *Sorting*: You can select fields to sort by and change the order of sorted fields
  - *Card view*: Choose the number of columns always visible or show the first column title.



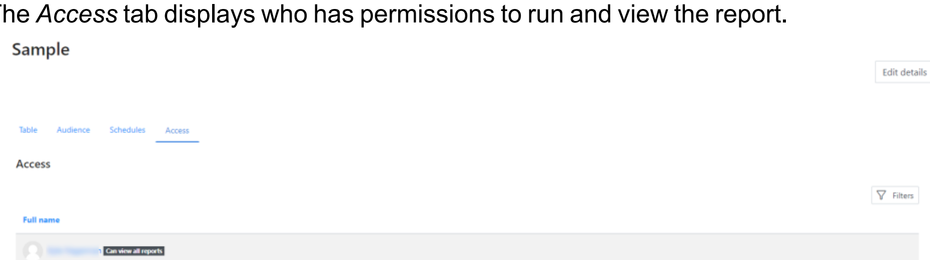
6. After selecting your data source and *Table* data, you can configure the audience for the report.



7. You can set the frequency of the report send from the *Schedules* tab.



8. The *Access* tab displays who has permissions to run and view the report.



For any custom created reports, you can:

- Change the name of the report
- Modify the configuration of the report
- Delete the report at a later date

This allows Administrators to re-purpose reports later.

www.fortinet.com