User's Guide

v4.2

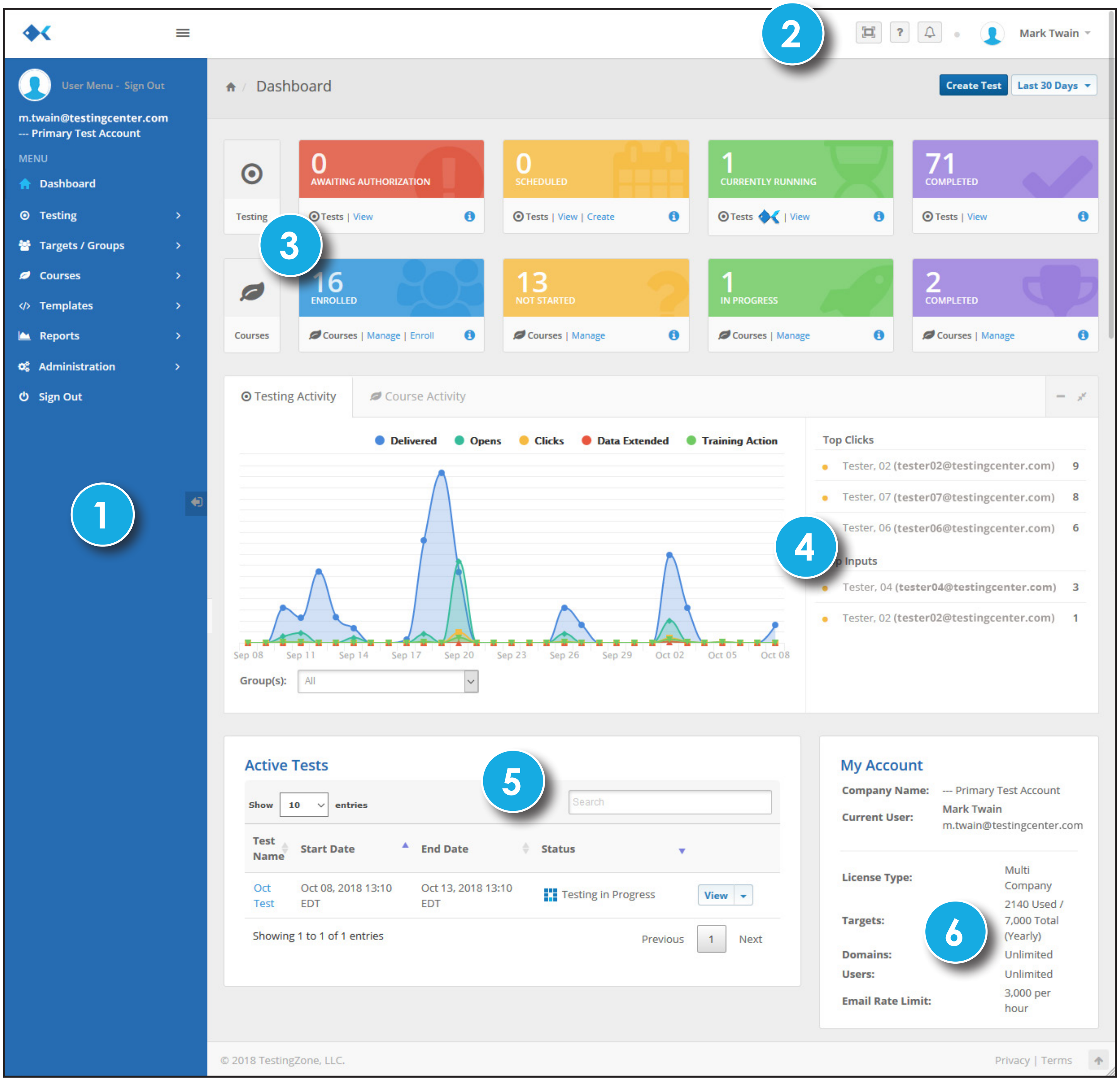
Updated: Feb. 18, 2019

Content

Dashboard

When you first log into the platform, you will be presented with your Dashboard. This central location gives you an overview of your account, let you view current and scheduled tests, and perform basic activities. All functions and features can be reached from the Dashboard.

Please reference an overview of our dashboard below, and the following pages for corresponding descriptions.



Dashboard

1 MAIN MENU

Dashboard returns you to this page.

Testing

Manage Target Domains allows you to manage your pre authorized domains.
Manage Tests allows you to view/manage all your tests.
Create Test launches the campaign wizard that will guide you through the process of configuring a phishing test.

Targets/Groups

Manage Targets allows you to view/manage all of your phishing targets (users).
Add Targets allows you to add targets manually, setup 3rd-party integrations (e.g., LDAP and SmarterU), or import from a CSV.
Manage Groups allows you to view/manage all of your phishing groups.
Add Group allows you to create a new group and setup special custom fields.

Courses

Manage Courses allows you to view/manage all of your training courses.
Create Course allows you to create your own custom phishing training course.
Enrollment allows you to manually enroll targets into training courses. This is non-campaign enrollment.
Course Library allows you to browse and copy pre-built courses to your account.

Templates

Manage Phishing Templates allows you to view/manage all the phishing templates you've created, or customized and added from our Template Library.
Manage Training Templates allows you to view/manage all the training templates you've created, or customized and added from our Template Library.
Create Template allows you to create a new template from scratch (either phishing or training).
Template Library allows you to browse, customize, and copy our system templates to your account. Whenever templates from the Library are customized or copied, they will be available in the appropriate 'Manage Templates' portion of this area.

Reports

Generate Reports allows you to generate reports based upon your selected criteria.

Administration

Account Information allows you to adjust account information like contact information and billing address.
Mange Users allows you to manage system users who have access to the Portal.
Mail Settings allows you to customize how emails are sent like default from address and custom SMTP settings.
API provides information about using the Portal's API features. This includes details API documentation and your API Token.

Sign Out logs you out of the system.

2 TOPBAR MENU

Allows you to enter full screen mode.

Clicking this will give you help and support. This box will expand to give you directions on how to contact support and showcase a Quick Help section that gives you detailed information that's specific for this page.

Shows System Alerts and Notifications.

Dashboard

3 SYSTEM SUMMARY

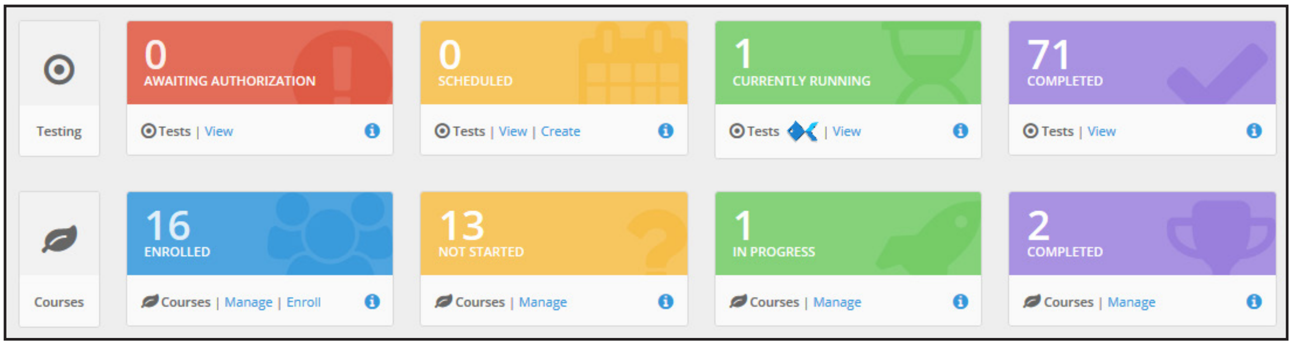
This section provides metric data about the different aspects of the system and provides quick links to related pages.

This section lets you know if you have any tests awaiting authorization.

This section counts how many tests have been setup, but have not yet started.

This section counts active, running tests.

This section counts tests that have already concluded.



This section counts how many targets are enrolled in training courses.

This section counts how many enrolled targets have not yet started their courses.

This section counts how many targets are currently taking a course.

This section counts how many targets have completed a training course.

4 Testing Activity

This section provides target activity over time, breaking it down into categories Delivered, Opens, Clicks, Data Extended (e.g., opened attachment, entered data, etc.), and Training Action. It will also list the targets who clicked and failed the most.

5 Active Tests

This section will list any tests that are currently running to give you quick access to statistics and reports.

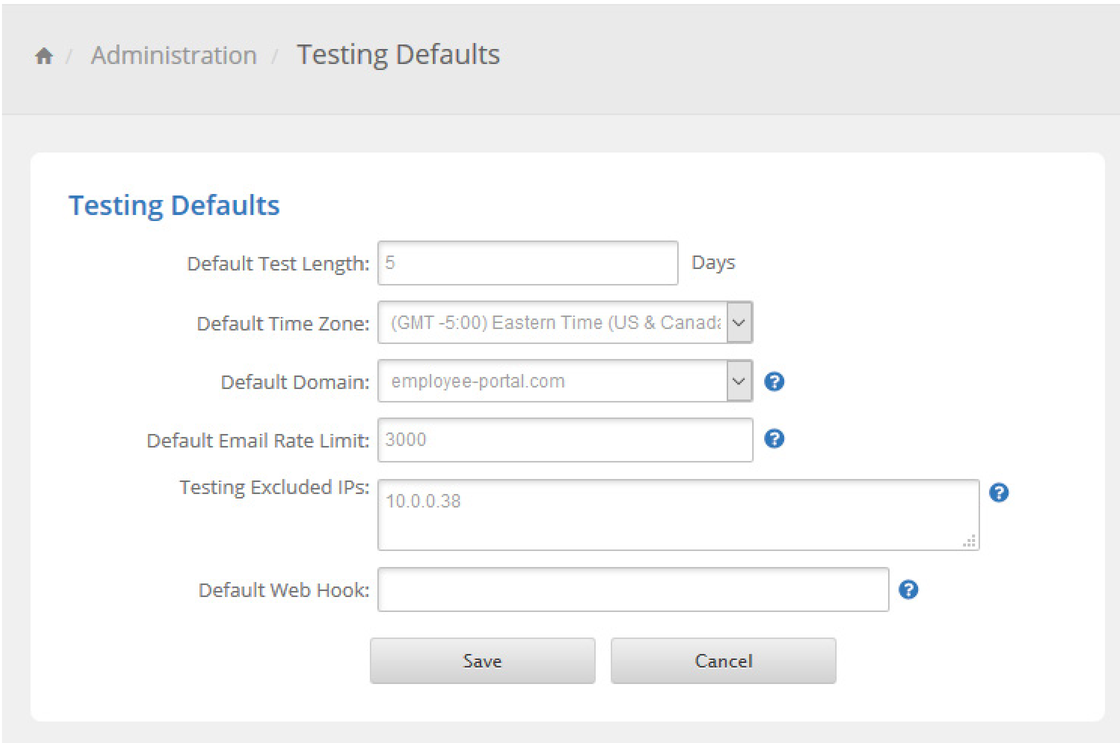
6 My Account

This section summarizes your account, such as the targets available. Any tests that are scheduled will show up in the targets pending.

Testing Defaults

Before configuring a test, you have the option to set various default items. These items are not required to be set before conducting a test, and some items can be modified during the test setup.

To change the default test settings, go to the Administration > Testing Defaults. If this menu is not visible, you do not have administrative rights to the account.



Default Test Length is how long you want your tests to run. This value will be populated in the test wizard but can be overwritten in the test setup.

Default Time Zone is what will automatically be used in the date/time dropdowns in the test wizard.

Default Domain is the default sending domain for your account.

Default Email Rate Limit is how many emails per hour that will be sent out for the **Immediate Test** type. The minimum send rate is 10 emails per hour.

Testing Excluded IPs are IPs that will be excluded from reports and statistical data.

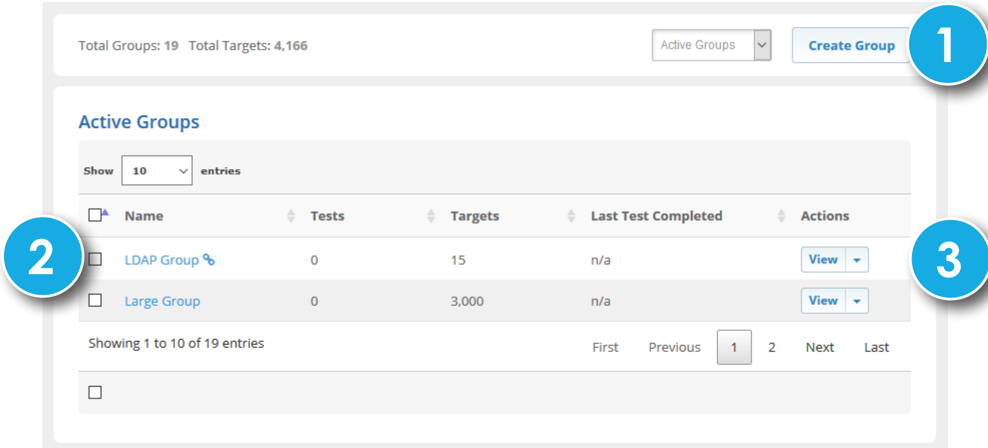
Default Web Hook is the url of an external file that will be notified of target actions. To use the web hook, you will need a receiving script setup to process the data on your end. The system will send the data in JSON format.

IP Whitelisting

Before running any tests, you need to whitelist the following IP addresses on your servers to ensure delivery:

64.191.166.196 **64.191.166.198** **64.191.166.199** **64.191.166.200** **64.191.166.201**

Manage Groups



1

Topbar Menu

The **Create Group** button takes you to the page to setup a new group.

The **Filter Dropdown** allows you to switch between viewing **Active** and **Inactive** groups. Inactive groups are hidden from the selection dropdowns through the platform's forms.

2

Groups

Each Group row provides summary information and quick links to access your detailed data. By clicking on the group's name you will be taken to the **Group Details Page.** This page provides you with summary data for all tests run on that group. If the group is integrated via a third-party (LDAP, Moodle, or SmarterU), there will be a link icon next to its name. Clicking on this link will re-sync the group with the external database.

3

Actions

View Details takes you to the **Group Details Page** where you get summary data or their group.

View Targets takes you to the **Manage Targets** page where you can edit target information.

Create Test takes you to the **Testing Wizard** to create a new test for the group.

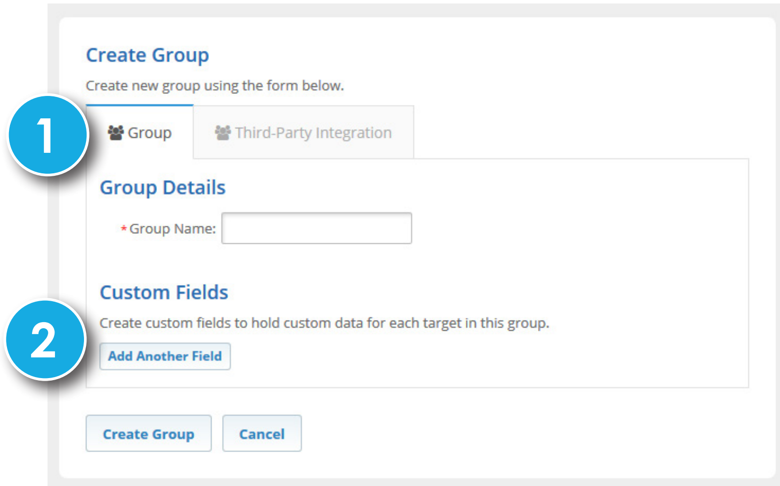
Advanced Reporting generates a **Summary Report** based on the group's data.

Sync Group re-syncs the group with the third-party integration (if one has been set up). This link is disabled if no third-party integration exists.

Edit allows you to edit the group name, authorize users who approve the tests, and 3rd party integration information.

Delete allows you to delete the group, its targets, and all its data.

Create Group



1

Group Tab

The Group tab contains the **Group Name** (the only required field) and the **Custom Fields** setup. If you want to sync the group with an external database (LDAP, Moodle, or SmarterU) you can use the Third-Party Integration tab to set it up (see the following pages for detailed information).

2

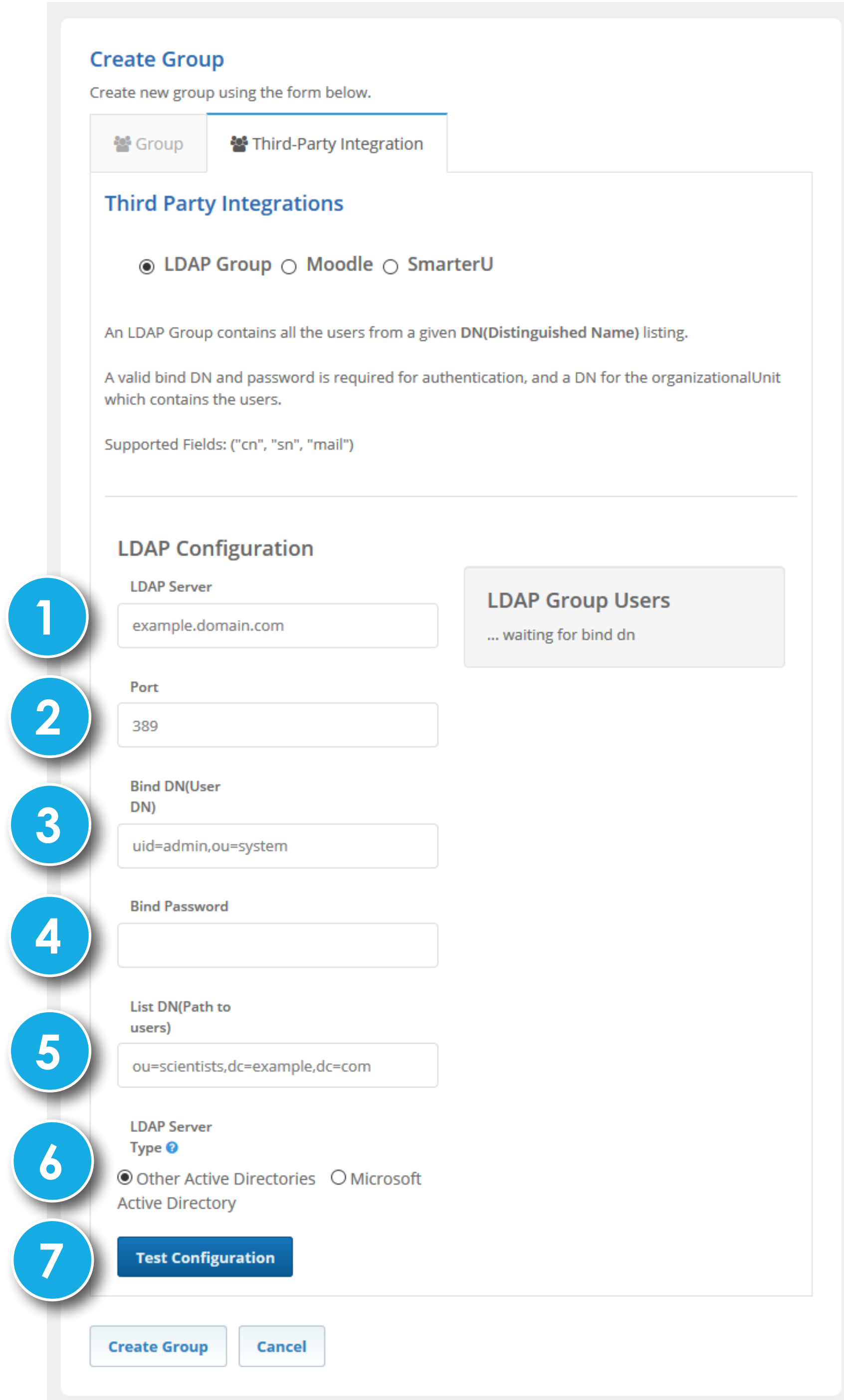
Custom Fields

Custom fields are any data (variables) that you want to associate/store in the system that is not already covered by our Pre-Defined System Fields (see chart to the right). Essentially, this is user data that will help with filtering users, parsing reports, and using variable data in phishing campaigns (e.g., office location, department head name, etc.).

Pre-defined System Fields

Name	Field
First Name	first_name
Middle Name	middle_name
Last Name	last_name
Email	email
Address Line 1	address_line_one
Address Line 2	address_line_two
City	city
State	state
Zip	zip
Country	country
Business Phone	phone_business
Business Fax	phone_business_fax
Mobile Phone	phone_mobile
Company	company
Title	title
Department	department
Sub Group	label
Manager/Supervisor	manager
Optional Field 1	optional_1
Optional Field 2	optional_2
Optional Field 3	optional_3

Third-Party Integration: LDAP



1 **LDAP Server**

The domain where your LDAP directoy resides.

2 **Port**

This is the port (389 is the standard) that external traffic uses to connect to your LDAP server. All traffic from our system will come from the following IPs:

64.191.166.196
64.191.166.201

3 **Bind DN (user DN)**

This is the distinguished name of the user with access to the directory.

Example:
cn=read-only-admin, dc=example, dc=com

4 **Bind Password**

The password of the user accessing the directory

5 **List DN (Path to users)**

This is the full path to the users you wish to import.

Example:
ou=scientists,dc=example,dc=com

6 **LDAP Server Type**

If you are using a Microsoft Active Directory make sure you check the appropriate radio button as it requires different search parameters. For all other LDAP servers use Other Active Directories.

7 **Test Configuration**

Once you have entered all the settings, click **Test Configuration** button to ensure the connection can be made. If a successful connection is made, a list of users will appear in the gray LDAP Group Users box.

Third-Party Integration: Moodle

1 **Moodle Server**

This is the domain where your Moodle server resides.

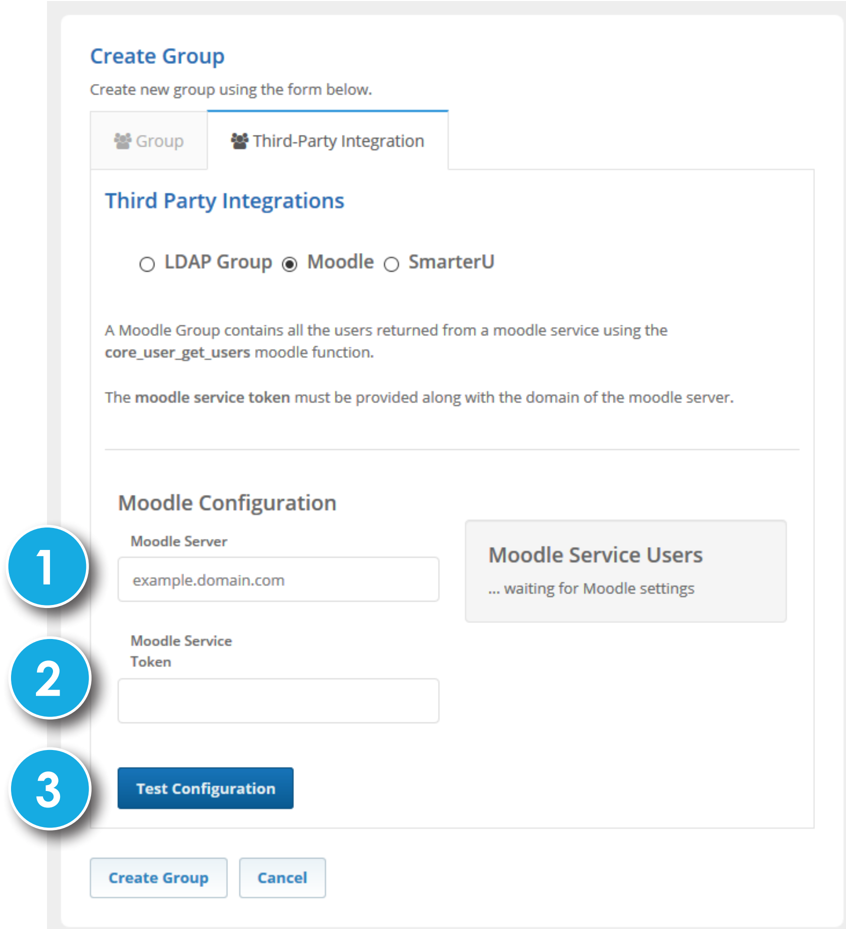
2 **Moodle Service Token**

This is the service token provided by Moodle for web services.

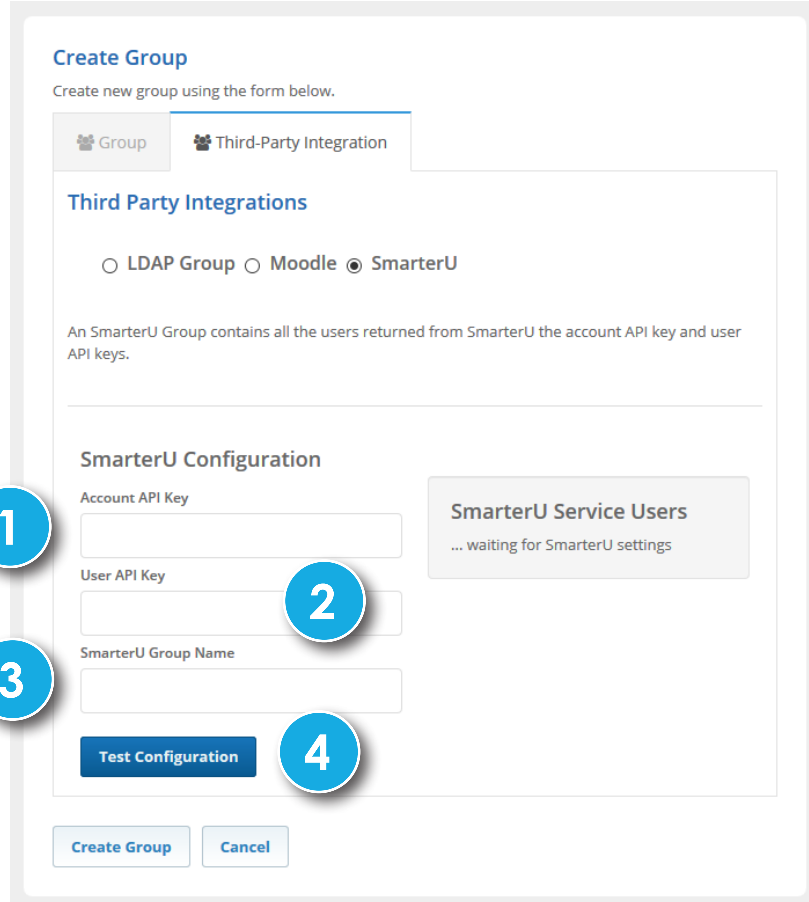
Reference your Moodle documentation on how to retrieve this token and enable web services.

3 **Test Configuration**

Once you have entered all the settings, click **Test Configuration** button to ensure the connection can be made. If a successful connection is made, a list of users will appear in the gray Moodle Service Users box.



Third-Party Integration: SmarterU



1

Account API Key

This is the API Key for the SmarterU account where the users you wish to import exist.

You can find the API Key at: Account Settings > API Setup.

You will also need to check "Allow API access for this account" and add the domain of our platform to the approved list.

2

User API Key

This is the API Key of the admin that has access to the users you wish to import.

You can find the User API Key at: User Admin > Users.

Select the user you want and the information is in the Login Information table.

3

SmarterU Group Name

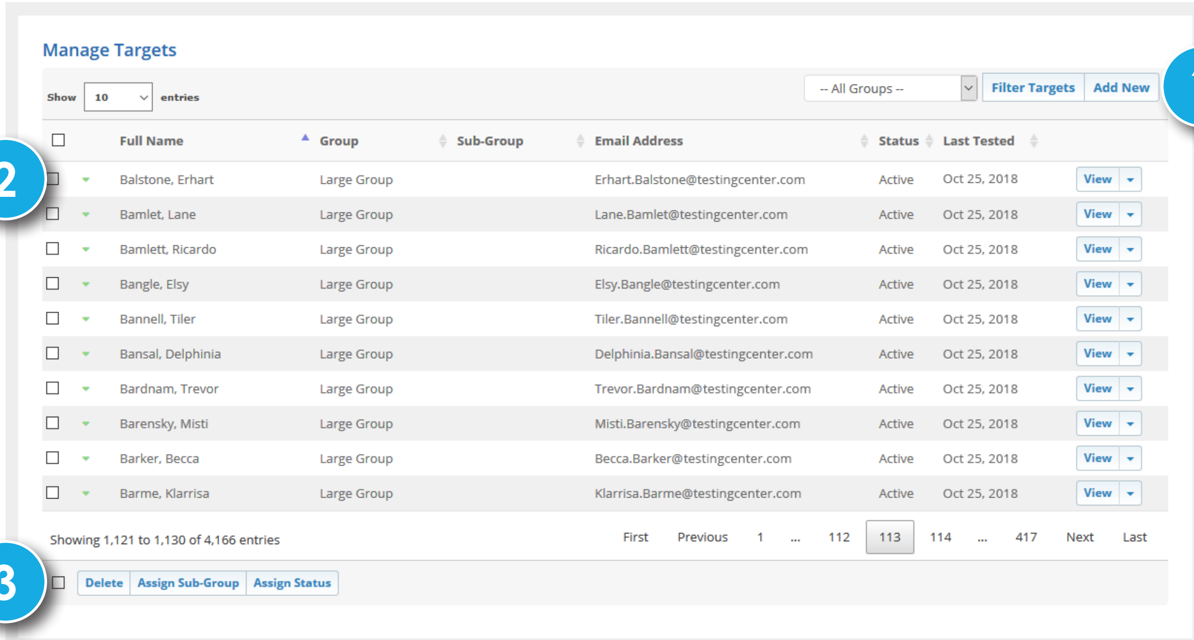
This is the Group Name assigned to the users you wish to import.

4

Test Configuration

Once you have entered all the settings, click **Test Configuration** button to ensure the connection can be made. If a successful connection is made, a list of users will appear in the gray SmarterU Service Users box.

Manage Targets



Manage Targets

Show 10 entries — -- All Groups -- | Filter Targets | Add New

	Full Name	Group	Sub-Group	Email Address	Status	Last Tested	
☐	Balstone, Erhart	Large Group		Erhart.Balstone@testingcenter.com	Active	Oct 25, 2018	View
☐	Bamlet, Lane	Large Group		Lane.Bamlet@testingcenter.com	Active	Oct 25, 2018	View
☐	Bamlett, Ricardo	Large Group		Ricardo.Bamlett@testingcenter.com	Active	Oct 25, 2018	View
☐	Bangle, Elsy	Large Group		Elsy.Bangle@testingcenter.com	Active	Oct 25, 2018	View
☐	Bannell, Tiler	Large Group		Tiler.Bannell@testingcenter.com	Active	Oct 25, 2018	View
☐	Bansal, Delphinia	Large Group		Delphinia.Bansal@testingcenter.com	Active	Oct 25, 2018	View
☐	Bardnam, Trevor	Large Group		Trevor.Bardnam@testingcenter.com	Active	Oct 25, 2018	View
☐	Barensky, Misti	Large Group		Misti.Barensky@testingcenter.com	Active	Oct 25, 2018	View
☐	Barker, Becca	Large Group		Becca.Barker@testingcenter.com	Active	Oct 25, 2018	View
☐	Barme, Klarrisa	Large Group		Klarrisa.Barme@testingcenter.com	Active	Oct 25, 2018	View

Showing 1,121 to 1,130 of 4,166 entries — First Previous 1 ... 112 113 114 ... 417 Next Last

Delete | Assign Sub-Group | Assign Status

1 Topbar Menu

The **All Groups Dropdown** allows you to specify a group from the main list. When a particular group is selected, an additional import button will automatically be activated.

The Import button is a quick import that allows you to automatically add any new targets in the CSV file. Using this will import/update any data that exactly matches the pre-defined system fields (see “Pre-defined System Fields” on page 8). Please note that this will not deactivate old users. For that option, you will need to use the Full Import tool on the Add Targets page.

Filter Targets allows you to narrow the target list based upon specific critera (i.e., Name, Email, Company, Title, Department, Manager/ Supervisor, Sub-Group, Country, City, State, Zip, and any Custom Fields you have set up.

Add New opens a pop up window for you to manually enter a new, single target.

Custom Fields

Custom fields are any user data (variables) that you want to associate/store in the system, that is not already covered by our Pre-Defined System Fields (See Chart to the Right). Essentially, this is user data that will help with filtering users, parsing reports, and using variable data in phishing campaigns (office location, department head name, etc.).

To utilize custom fields, simply click on the Add Another Field button and fill in the field’s name.

2 Target Row

This contain basic information about the target, their current status in the system, and the last time they were tested.

Actions

View Details takes you to a page that summarizes all of the targets testing data.

Edit opens a pop up window that allows you to edit all the information associated with the target.

Delete allows you to delete the user from the system, along with any associated data.

Mass Action Options

3

Delete allows you to delete all the checked targets and their associated testing data.

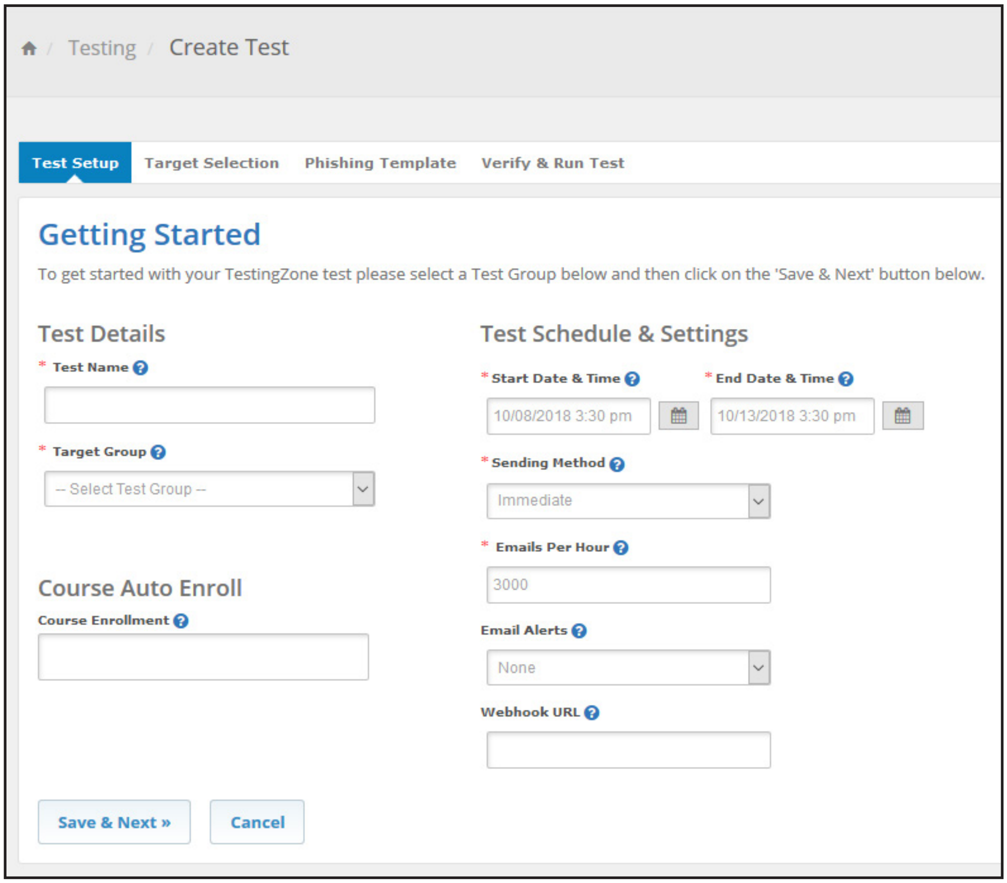
Assign Sub-Group allows you to set the Sub-Group for all the checked users.

Assign Status allows you set the status of checked users to Active or Inactive. An inactive status causes the targets to not be listed within the **Testing Wizard** and other, select locations in the platform.

Test Creation

Step 1

From the Getting Started tab you will give the test a unique name to identify it in the system later, select/create a group, select courses to auto enroll failed targets to, and set up basic scheduling information.



If you create a new group, you will add targets on the next screen.

Course Auto Enroll

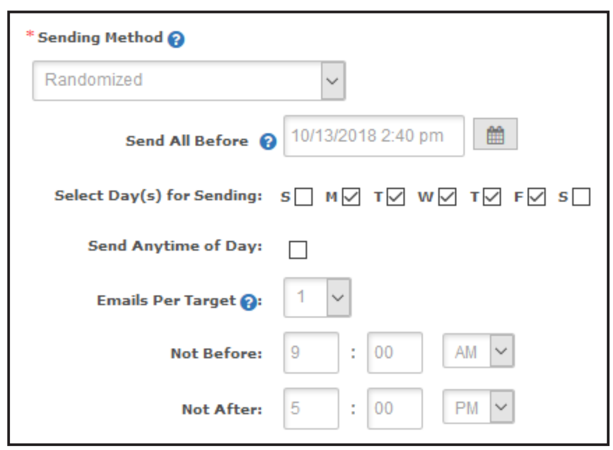
If your account has the Course module activated, you will have the option of adding courses to the test. You will need to have courses already created or grabbed from the Course Library before beginning the Test Wizard.

Test Schedule

Click on the Calendar icons to change the start and end dates/times for the test. Timezone settings are also located here.

Immediate tests send out the emails immediately upon wizard completion/test authorization. Based on the Emails Per Hour rate, the system will continue sending emails until all have been sent out.

Emails Per Hour is how many emails will be sent out each hour until the sending is complete. The minimum rate for the system is 10 emails per hour.



Randomized tests send out emails based upon the scheduling conditions you set up.

Send All Before is the absolute latest that any email in the test will be sent. Our system will perfectly schedule/divide all emails to be sent between the ‘Start Date & Time’ and ‘Send All Before’ date and time.

Select Day(s) allows you to specify which days of the week to send emails.

Send Anytime of Day determines what time of day the emails will be sent. If checked it will send out emails at equal intervals throughout the day and night. If not checked, Not Before and Not After time input fields will appear to restrict when the system will send emails.

Emails Per Target is how many test emails will be sent to each target. You will need to select the same number of templates to ensure a different email is sent each time.

Test Creation

Step 2

The Target Selection menu allows you to select the specific targets to be included in the test. To aid in selecting appropriate targets, the date of the last test is provided. Targets may be entered manually or imported via a .csv file. To import, headings in the files must be equal to the headings for each field in the system.

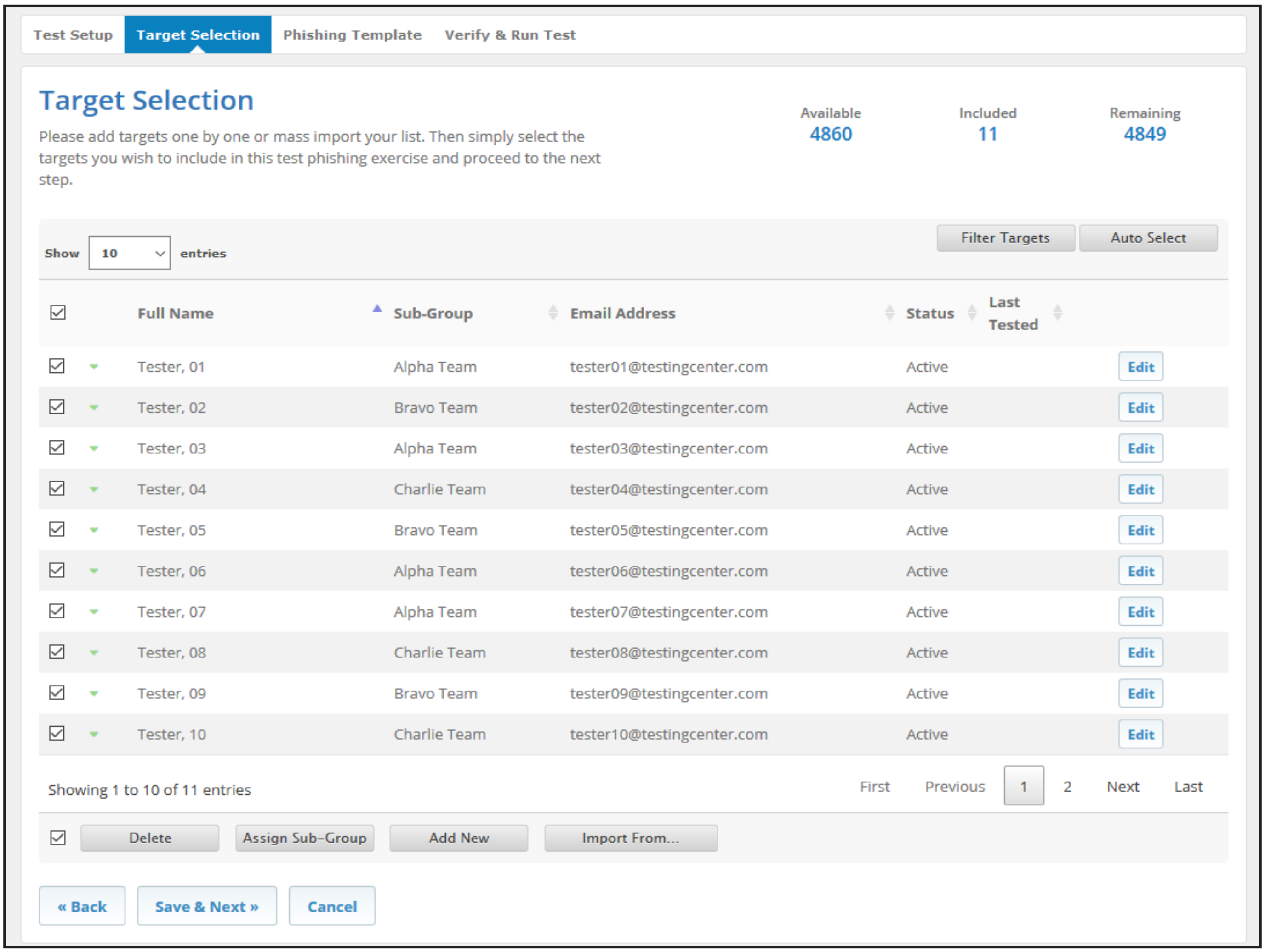
In order to run a test, there must be at least as many targets "available" as are included in the current test.

Using the **Filter Targets** button, you can also filter the target list by name, email, company, title, department, manager, sub-group, country, city, zip, last tested, and any predefined custom fields.

Using the **Last Tested** dropdown, you can quickly isolate users that have Never Been Tested, Previously Tested, Previously Failed, and Not Tested in 12 Months.

If you have active filters, only those targets matching your filters will be considered.

With the **Auto Select** button, you can randomly select targets using a Sample Selection Percentage (ie 50%), Sample Selection Number, or by Confidence Level.



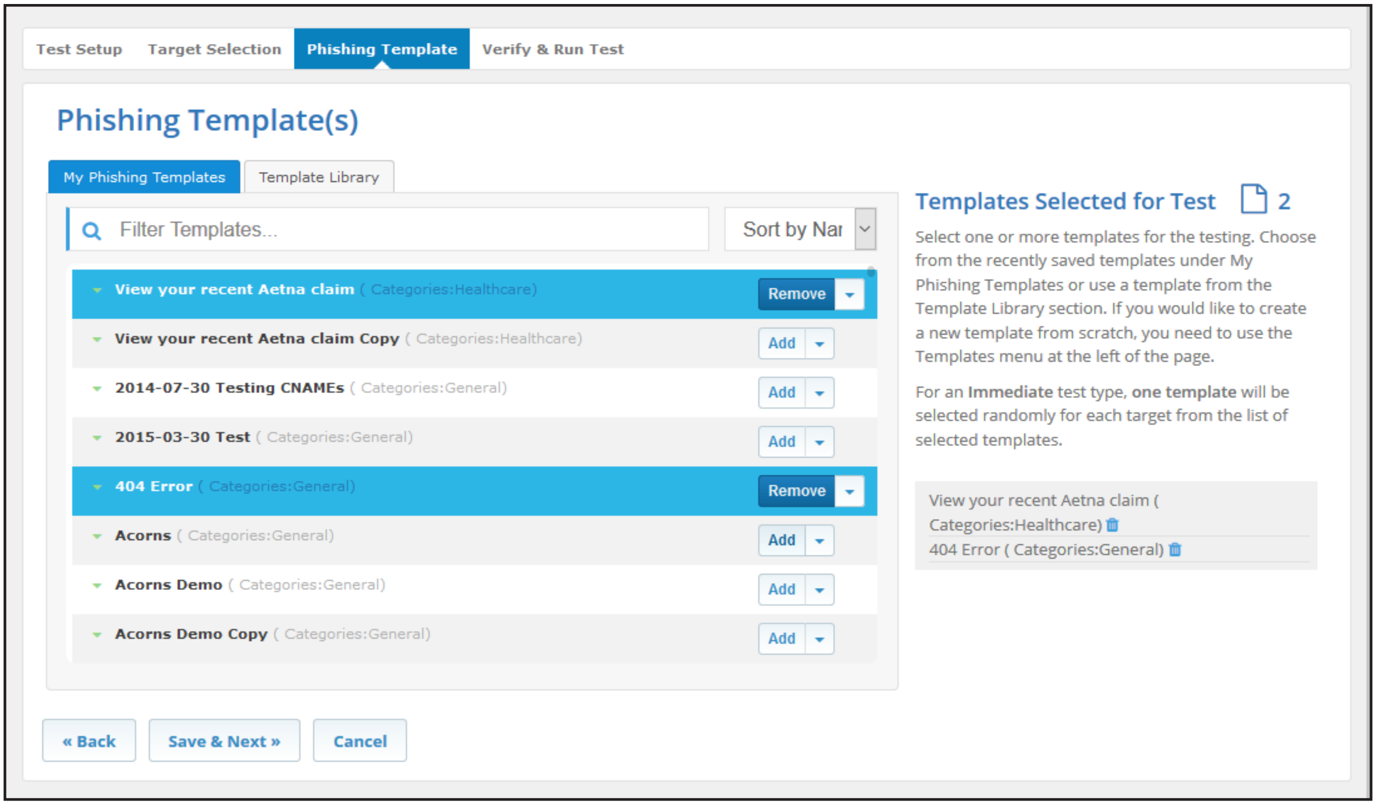
Test Creation

Step 3

My Phishing Templates are all the phishing templates you've created, or customized and added from our Template Library.

The Template Library are those provided by the platform. You can customize these templates as needed. Once used, they will be in the Manage Templates section.

Once selected, the templates you have chosen will be highlighted in blue and will be listed in the gray box on the right of the screen.

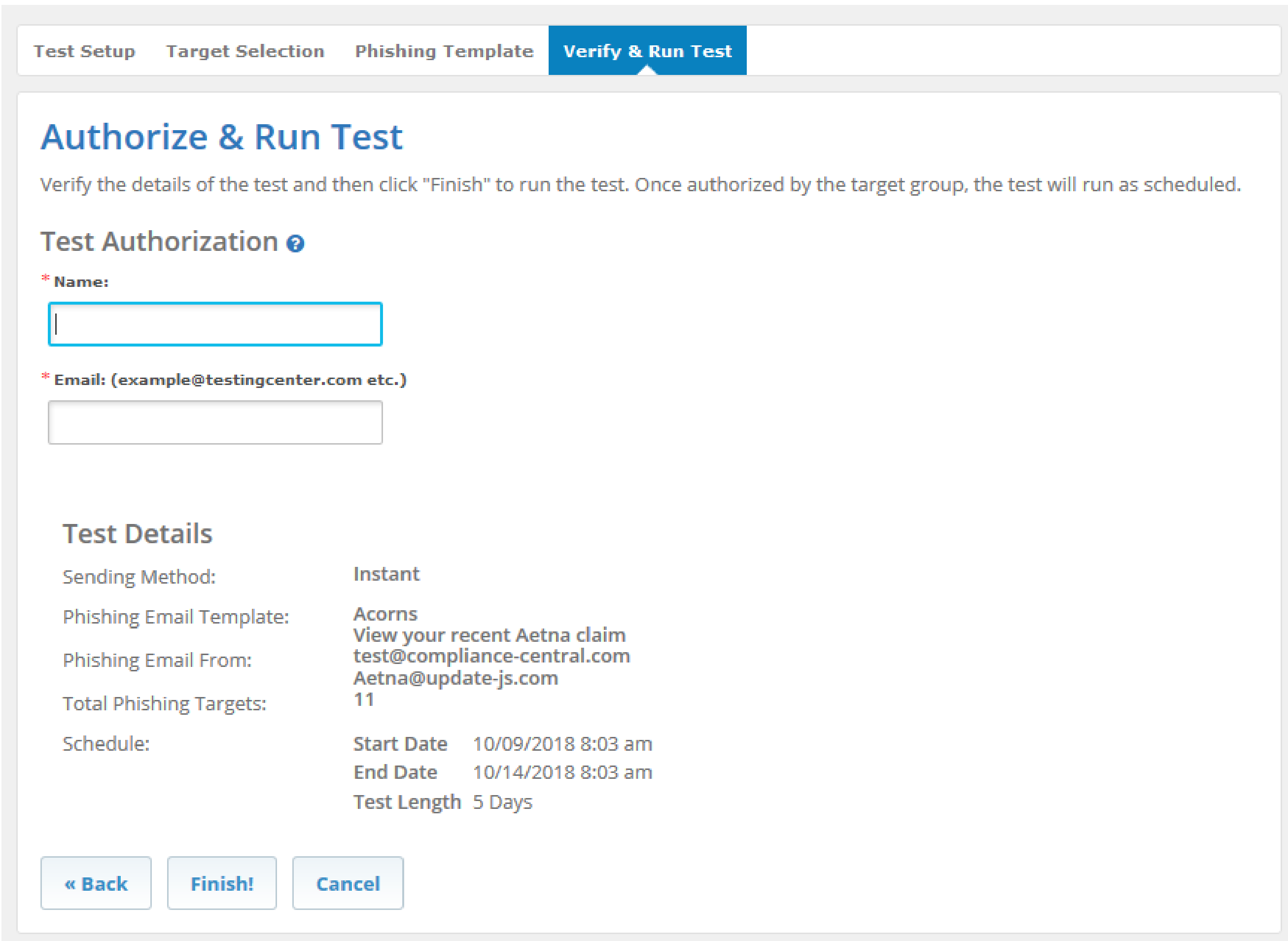


Test Creation

Step 4

The Test Authorization is where an individual from the target group is identified who can authorize the test to occur. This authorization is required for every @domain included in the test. The reason for this authorization is to ensure that the system is not abused by testing entities that do not know the test is going to occur. Until this authorization is received, the test will be set as Awaiting Authorization on the Dashboard. Once authorized, the test will run as scheduled. If the test time period ends without authorization, the test will be listed as Expired.

Additionally, you can pre-authorize domains so that you no longer need to send a test authorization for each phishing campaign under Manage Target Domains. For instructions, see the following page.

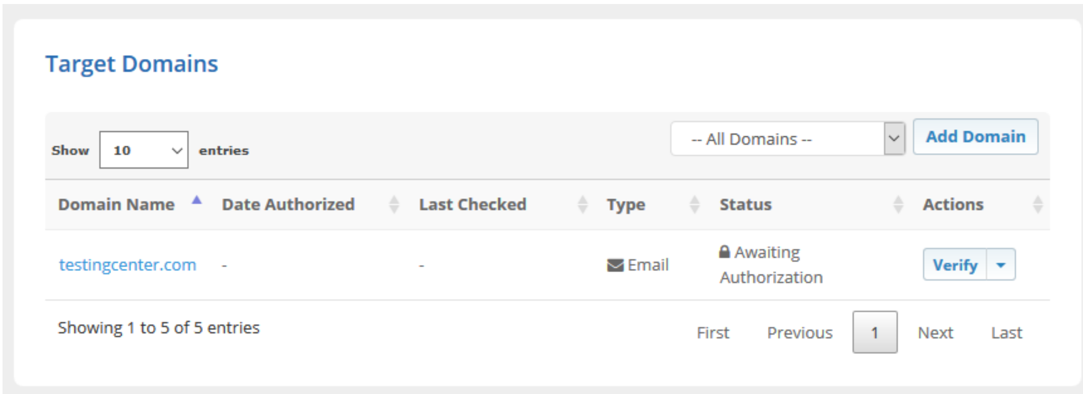


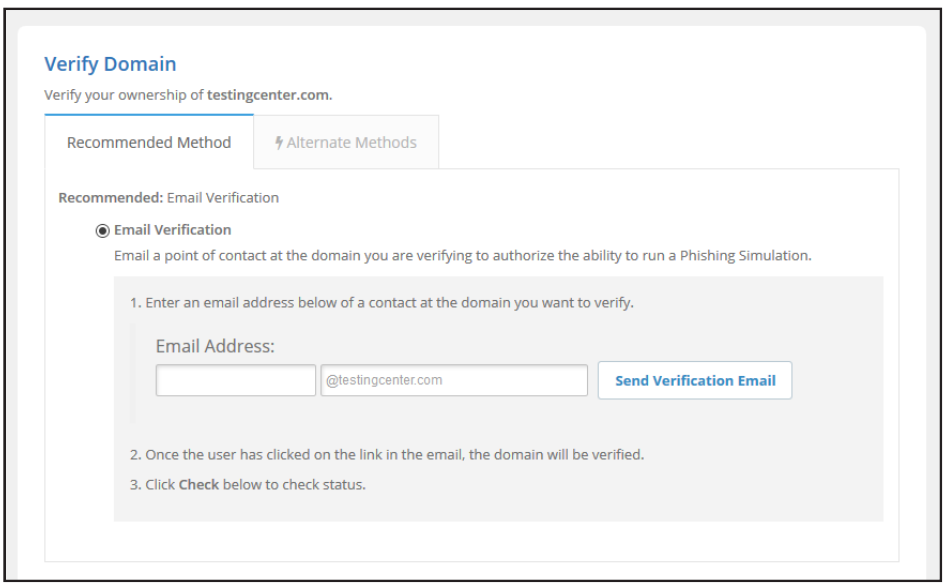
The page also provides a summary of the test configuration. If accurate, click finish and the test will run as scheduled. Note: The test must be authorized before the target domain before the individual targets will receive an email.

How to Pre-Authorize Domains

Location: Testing tab > Manage Target Domains

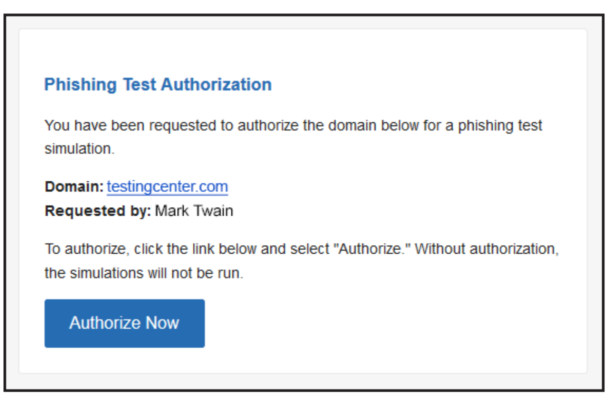
Pre-authorized domains allow you to bypass sending an authorization email for every domain you are testing. To add a new domain, simply click the Add Domain button. A pop up window will appear where you can enter the domain to be added.

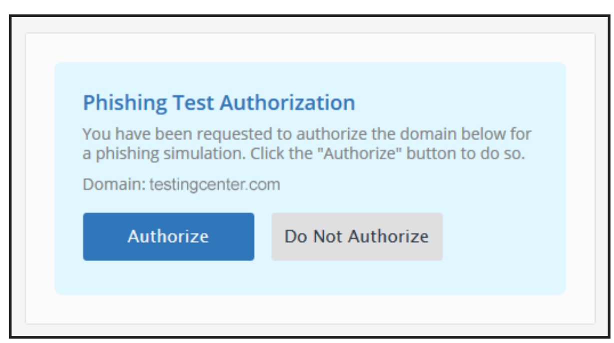




Once added, you will be transfered to the Verify Domain page where you can select the method you wish to use in order to verify the domain. There are four methods to choose from: email (recommended), an HTML tag, an HTML file, and a manual authorization form. Simply enter the authorizer's email address and click Send Verification Email.

The recipient will receive an email similar to he one on the left. After clicking Authorize Now, they will be taken to a page similar to the one on the right where they approve the authorization.





How to Pre-Authorize Domains

The remaining three methods are list below with instructions on how to implement them.

◉ **HTML Tag**

Add a meta tag to your site's home page.

1. Copy the meta tag below, and paste it into your site's home page. It should go in the **<head>** section, before the first **<body>** section.

```
<meta name="pbox-site-verification" content="PB-141255102817" />
```

2. Click **Verify** below to verify domain.

◉ **HTML File**

Upload an HTML file to your site.

1. Download this HTML verification file. [pbox141255102817.html]
2. Upload the file to testingcenter.com.
3. Confirm successful upload by visiting
4. Click **Verify** below to verify domain.

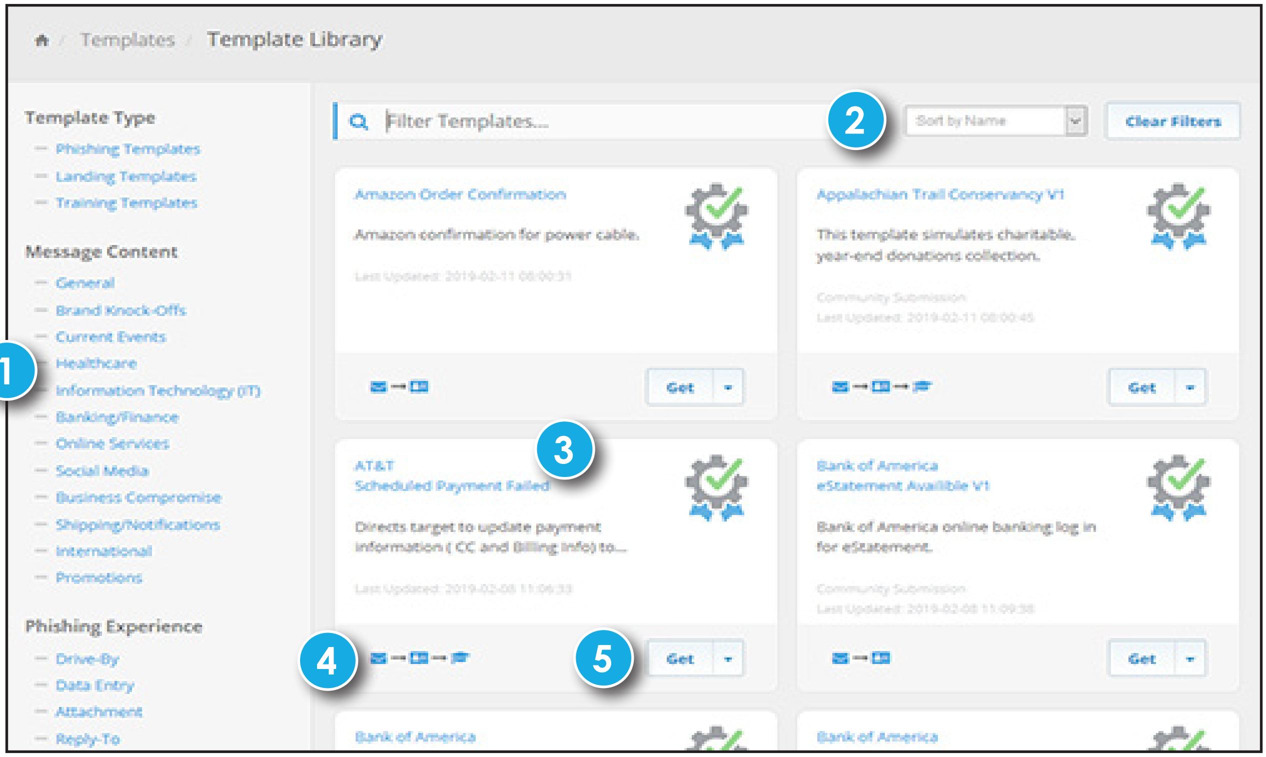
◉ **Manual Domain Authorization Form**

Download a PDF of the Manual Authorization Form.

1. Download the Manual Domain Authorization Form, click here.
2. Fill out form and email to support@phishingbox.com

After you submit the form it will take up to 24-48 to process.

Template Library



1 **Template Categories**
The Template Library has a host of templates, which is constantly updated, and is broken down into specific categories on the left. The listings are dynamic, so if you click on a specific category, the page will filter according to your selection. You can select as many categories as you like and the page will automatically adjust based on your selection. The categories are broken into several groups based upon content, phishing experience, target department, and nationality.

2 **Filter Templates**
This function will allow you to sort the templates by 'Last Updated' and 'By Name,' as well as dynamically search for templates using the search bar. The search is responsive, so you don't have to type in the exact name of the templates you're looking for. For example, if you're looking for an Office 365 template, you only need to type a couple letters for the system to generate results. These filters work with the category selection on the left and can be combined to narrow down the templates to exactly what you are looking for.

3 **General Template Listings**
Each template entry contains an overview with the name of the Template, a brief description, and the date it was last updated in our system.

4 **Phishing Progression Diagram** You will also notice icons representing the different steps in this phishing experience. The first icon in the chain tells you what kind of template it is: Email, Landing Page, or Training Page. The icons that follow show you the rest of the phishing progression for the template. The is a URL Replication and is a URL Redirect. Hovering over any of these icons will tell you the name of the template (or URL). Clicking will give you a preview of what the template looks like.

4 Utilizing the Get dropdown will allow you to Preview the Phishing Email, Preview the Landing Page, and Preview the Training Page for this template. This works the same as clicking the Email or Landing Page icons. Selecting 'Get' will allow you to fully customize the email and landing page.

Create Template

1 **Template Name** is how the template will appear in drop down lists and selection windows, so make sure you use a description name.

2 **Template Description** is optional text where you can describe the template in more detail.

3 **Template Categories** help sort and filter templates in the system.

4 **Template Type** is the type of template you want to create.

Email Template is the phishing email that targets will receive in their inbox.

Landing Page Template is a web page that the target will be taken to if they click a link in the phishing email. These pages are meant to phish the target further with a form, download, or replicated URL.

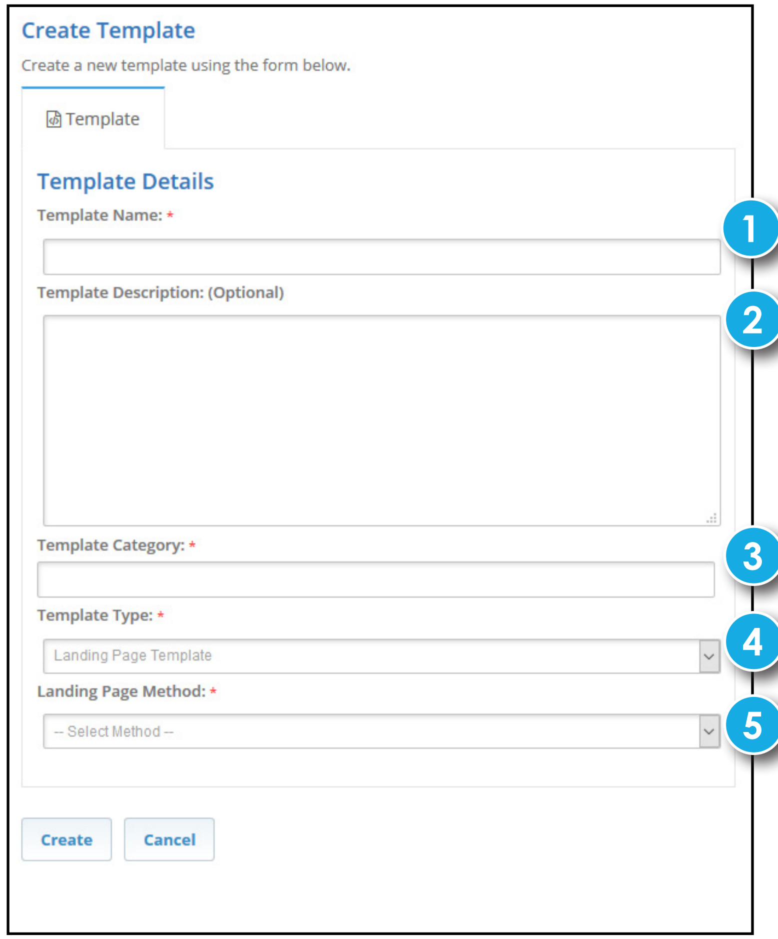
Training Page Template is a web page designed to provide targets with phishing training. These templates can be attached to either emails or landing pages depending on the phishing progression you wish to use.

5 Landing Page Method will appear if you are making a landing page. It is the phishing hook used on the Landing Page.

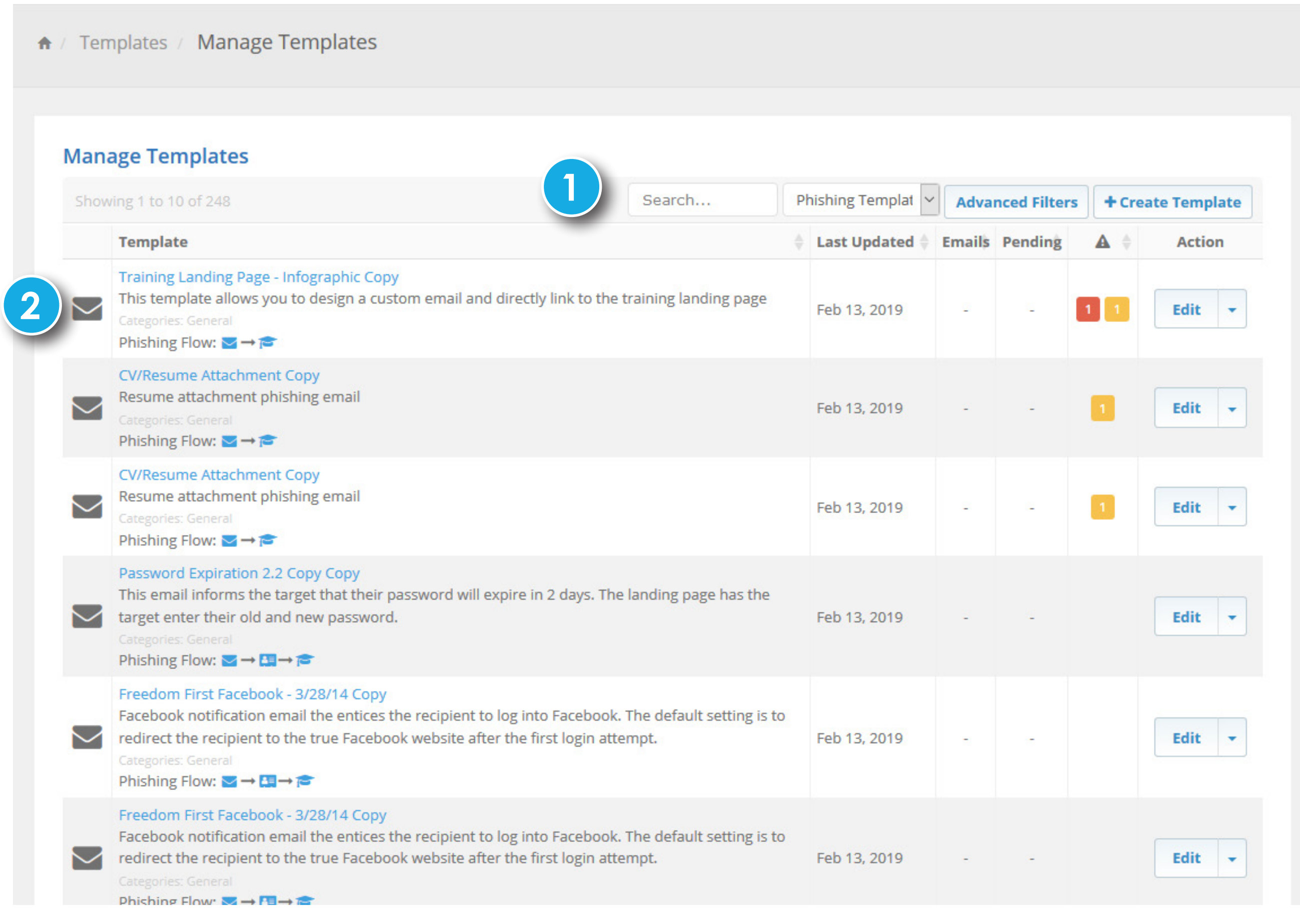
Data-Entry is the most basic phishing method and will simply collect data from the targets using a form.

Download will turn on additional fields to allow you to customize a file download.

URL-Replicate allows you to replicate another website as your landing page. You will get an *URL to Replicate* field to enter the website you want to replicate. The Landing Page editor will turn off since the system will build the HTML for you.



Manage Templates



1 **Template Top Bar** contains several important items.

You can use the search bar to filter based on any of the text in the *Name, Description,* or *Categories*.

By default, the Manage Templates page is set to show only the Email Templates. If you wish to see Landing Page or Training Page Templates you can use the drop down menu.

Advanced Filters — *Advanced Filters* button opens a window that allows you to filter the templates based upon the category groups in the system: Content, Experience, and Target Department.

+ Create Template — The *Create Template* button will take you to a new page to create a template.

2 **The Template Row** provides you with useful information about each template.

The first column displays an icon identifying the template type: Email, Landing Page, or Training Page.

The **Template** column shows the template name, description, categories, and phishing progression (see Template Library for more details).

The **Last Updated** column shows the date the template was last saved.

Based on which type of template you are viewing the next few columns can change.

The **Emails** column is how many phishing emails used this template.

The **Pending** column is how many pending (waiting in the queue to be sent) phishing emails are using the template.

The **Temps** column is to how many other templates the current template is attached.

The ⚠ **(Errors & Warnings)** contains icons (errors in red, warnings in yellow) that will notifiy you if there are any problems with the template that could cause problems when sending a phishing campaign. Every time you save the template the system will scan the template for these and update the template with the appropriate messages. These warnings will also be displayed when creating a test so that you don't accidently use a template that has errors. This section will appear on each of the tabs of the editor since each element is its own template.

The **Actions** column provides useful links to manage your templates.

The **Edit** button (and link in the drop down menu) will open the template in the Template Editor along with any other attached templates further down the progression.

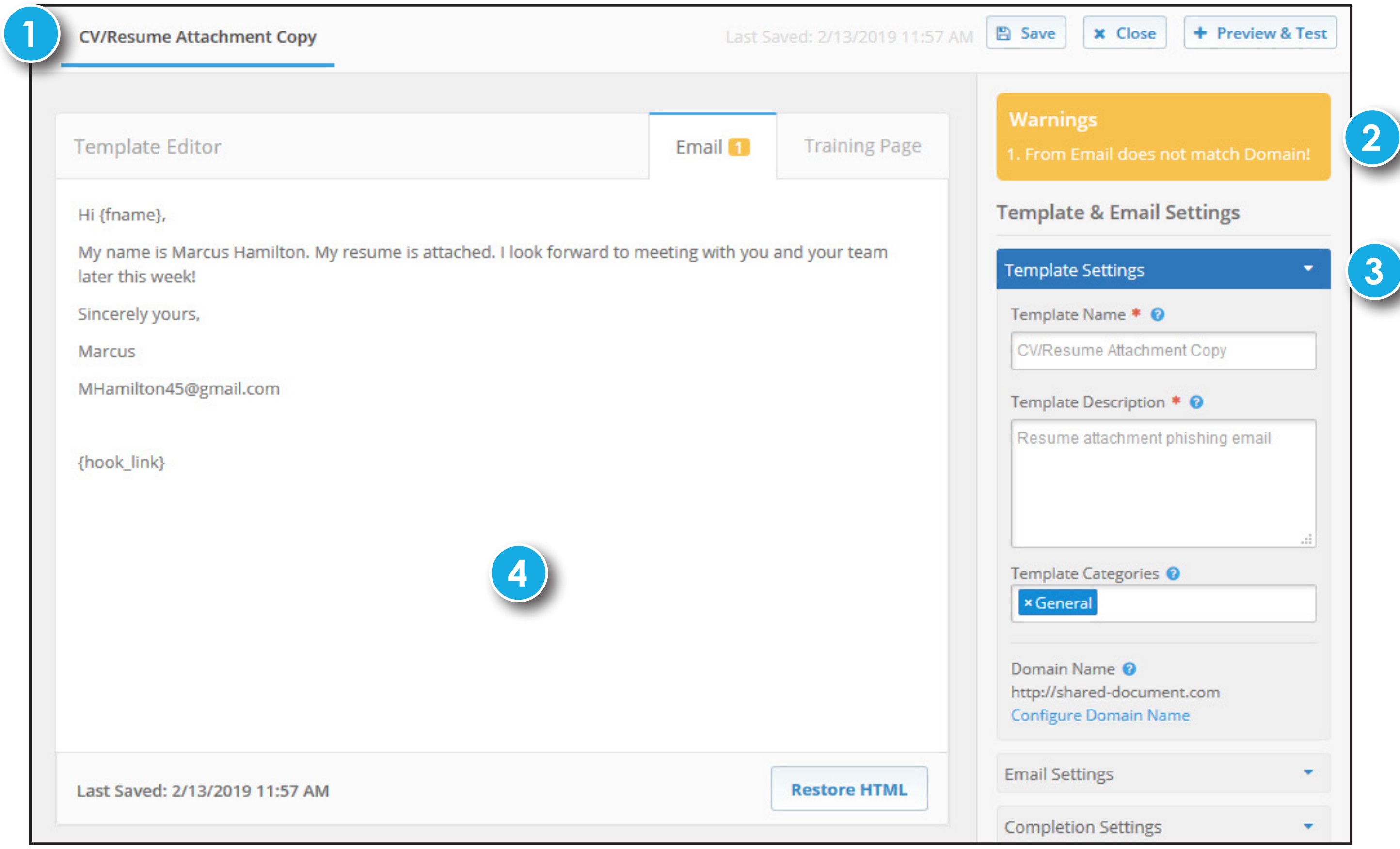
The **Preview** links will open the appropriate templates in either a pop-up window or new tab.

The **Submit Template to Library** link will submit your template as a candidate to go in the Template Library for others to copy and use.

The **Copy** link will create a copy of the template (all attached templates will be maintained, i.e., they won't be copied).

The **Delete** link allows you to delete the template (only a template with no connections to other templates can be deleted)

Customizing Templates - Email Tab



1 **Template Top Bar** contains several important items.

Save — You will need to click the **Save** button in order to retain any changes you have made while editing, this includes any information entered on a pop up window.

× Close — Clicking the **Close** button will return you to the Manage Phishing Templates page.

+ Preview & Test — In order to send yourself a preview email of the template use the **Preview & Test** button

2 **Errors & Warnings** contains sections that will notifiy you if there are any problems with the template that could cause problems when sending a phishing campaign. Every time you save the template the system will scan the template for these and update the template with the appropriate messages. These warnings will also be displayed when creating a test so that you don't accidently use a template that has errors. This section will appear on each of the tabs of the editor since each element is its own template.

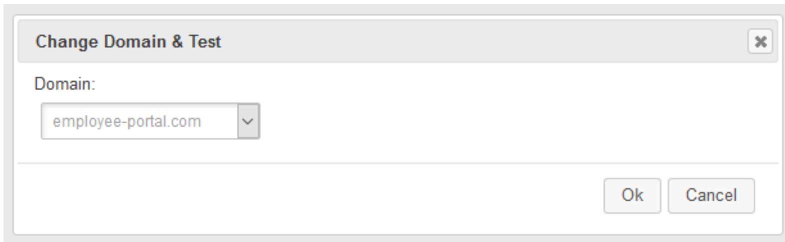
3 **Template Settings**

Template Title and Template Description Inputs are where you can modify the title and description of the template to better identify it elsewhere in the portal.

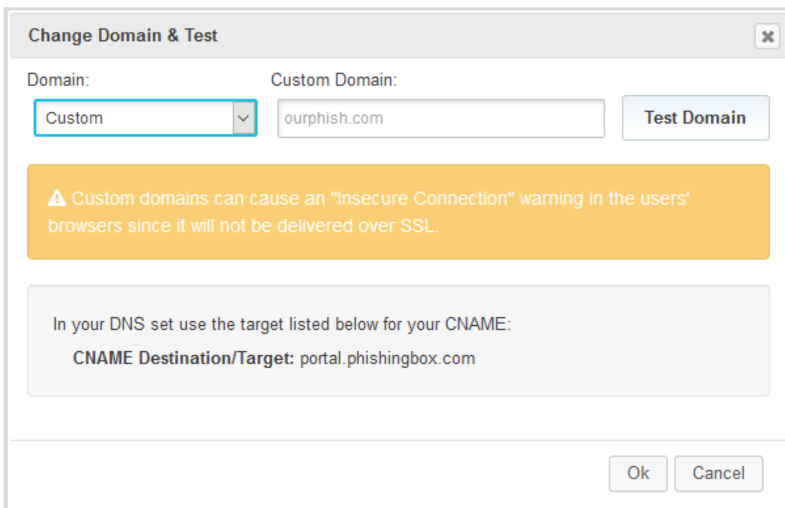
Template Categories allow you to classify the template to aid in filtering and searching elsewhere in the portal.

Customizing Templates - Email Tab

Domain Name is the domain of the phishing landing page that the target will be taken to if they click on the link in the phishing email. You have the option to use one of the system domains (which will be delivered over a secure HTTPS connection) or your own custom domain (delivered over an HTTP connection).

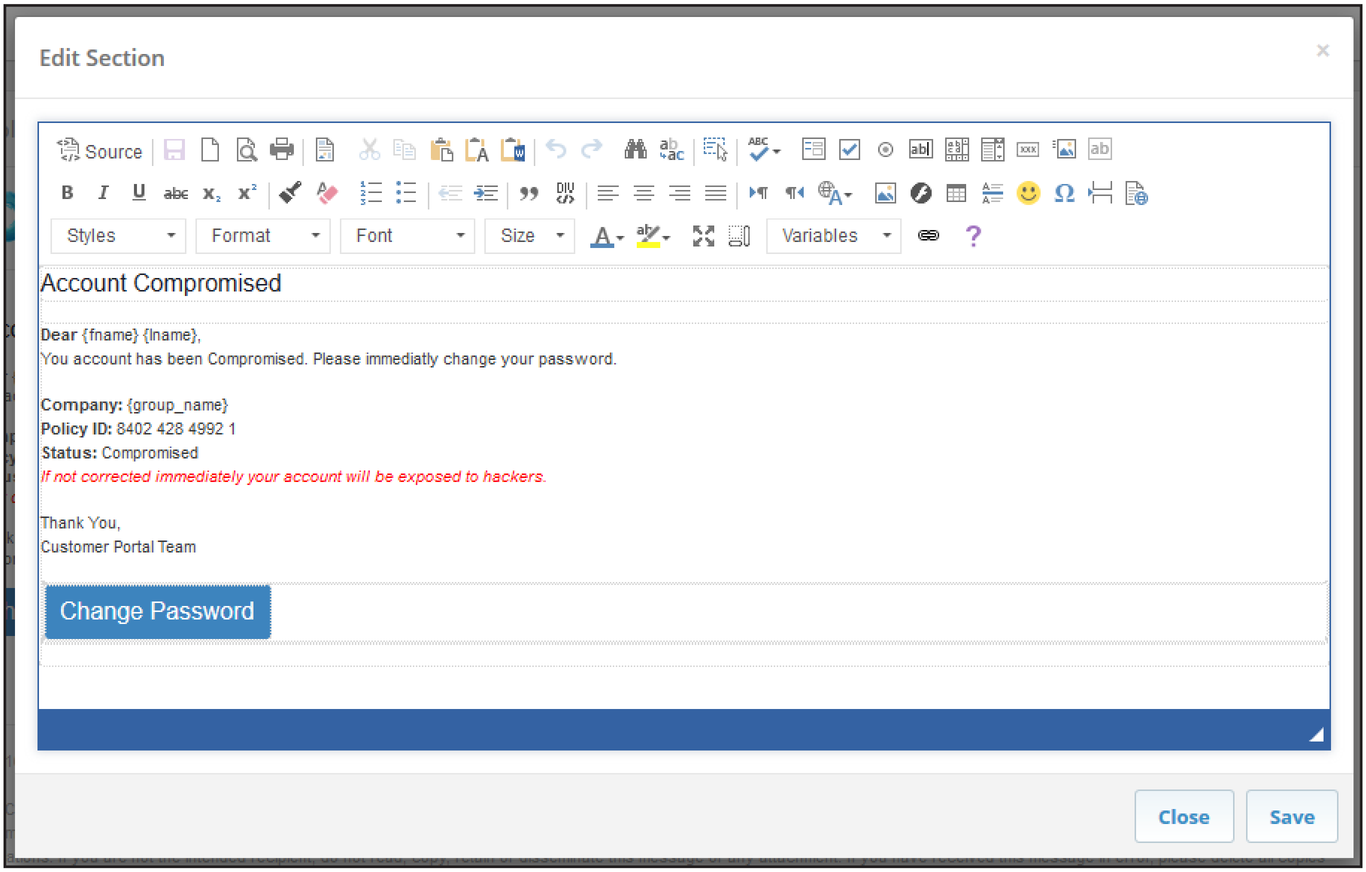


In order to use your own custom domain, you will need to set portal.trainingcenter.com as the target for the CNAME in your DNS configuration and pass the connection test on the Change Domain pop up window.



Customizing Templates - Email Tab

4 **Email Editor** allows you to edit the content of the email through a WYSIWYG editor. Editable sections will be highlighted by a dashed orange box when you roll over the section. A pop up window will open with the content. Any links you want to redirect to the template's landing page (and be tracked) should use {hook_url} as the URL. The system will replace this tag automatically with the appropriate link.



When editing the template, the Variables dropdown allows you to select items that will be replaced in the actual test email. These include, but are not limited to, such items as the target's name, or optional group and target fields. See the appendix for a listing of available variables.

The "hook_url" can be used in place of the "hook_link". This option will show the entire url in the email. This is also used if you want a clickable image.

Images may also be clickable for tracking purposes, simply place {hook_url} in the Image URL field.

Customizing Templates - Email Tab

1 **Email Settings** allows you to set the from name, from email, reply-to email, and subject line for the phishing email.

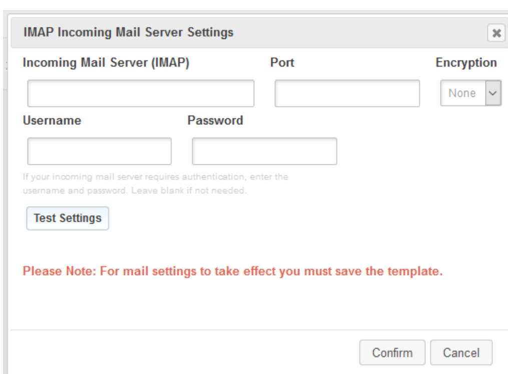
2 **Completion Settings** allows you to set up the next step in the phishing progression.

> **Landing Page** allows you to select a landing page to redirect the target to where they can continue to be phished, either your own custom page or a system library page. There is also an option to copy the current landing page (if one is already selected) or create a new page from scratch.
>
> **Training Page** allows you to select a training page to redirect the target to, either your own custom page or a system library page. There is also an option to copy the current training page (if one is already selected) or create a new page from scratch.
>
> **URL Redirect** allows you to redirect the user to any URL you choose.

The appropriate secondary fields you will need to fill out will appear based upon your selection in *Landing Page Options*, either a drop down to select the landing/training page you want or a text input to enter a URL.

3 **Custom Mail Servers** allow you to configure you own mail servers to send the test emails (the SMTP settings) or a custom inbox (the IMAP settings) to receive reply-to emails that the system can scan and log.

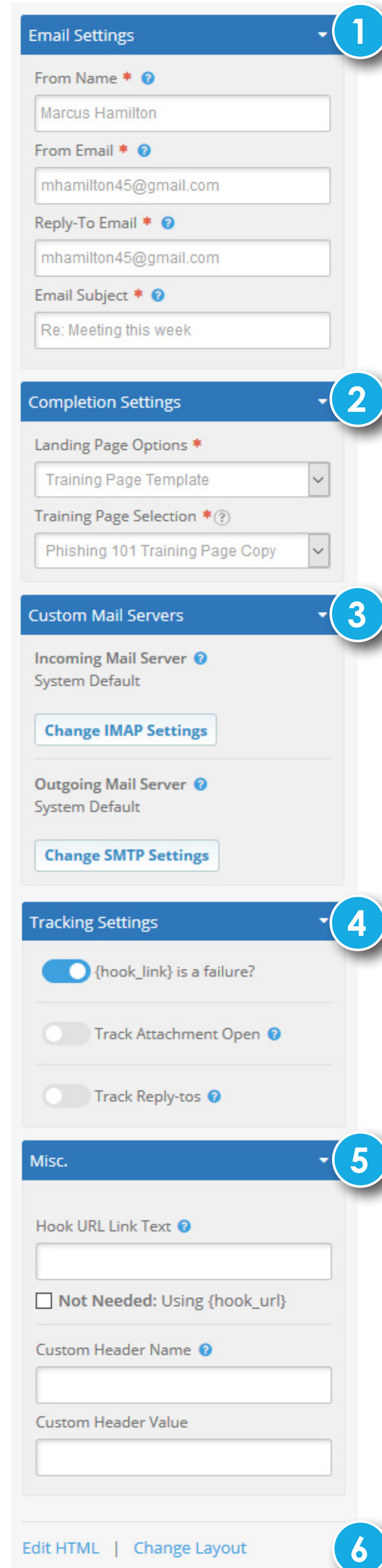
For each you will need to know the host, port, username, password, and encryption type. Once your settings are entered, you will need to click the *Test Settings* button to verify that the system can connect.



4 **Tracking Settings** allow you to adjust how failures will be tracked for the template.

The {hook_url}/{hook_link} is how the system tracks a "Click" and the way you get your targets to the next step in the phishing progression. Unless you only want to track email replies, your email **MUST** contain one of these customization tags in the email body.

> **Should {hook_link} click be a failure?** allows you to determine if clicks in the email should be logged as failures or not.
>
> **Hook URL Link Text** is the text that will appear in the email link.
>
> **Not Needed: Using {hook_url}** allows you to use the url as the text instead.



Customizing Templates - Email Tab

Track Attachment Open allows you to add an attachment to your email that can be tracked in the system. In order to use this option, you must use one of the predesigned files from the system (either Word or Excel). You can download these files directly from the template editor. These files contain special tracking keys that the system is listening for. You are free to add your own content to these files, however do not modify the {{tracking_key}}. For word docs, the key must be on its own line at the bottom of the page. For excel files, the {{tracking_key}} must be in sheet 1 in cell A299. Save as docm or xlsm. Once you have finished editing your files you can upload them using the Add Attachment button.

Track Reply-tos allows you to track email replies to your phishing emails. In order for this to work you will need to set up an incoming mail server (IMAP) for the system to monitor. The system will log in periodically and scan for emails. To enter your IMAP creditentials into the system, click on the *Change Outgoing/ Incoming Server* link and a pop up window will appear that will allow you to test the connection.

Track Email Open (DEPRECATED) has been removed from the options. Now all email opens will be tracked by default.

5 **Misc. Settings**

Hook URL Link Text allows you to customize how the URLs are displayed in the emails. By entering text in this field you can customize how the anchor tag will read. Additionally, you can choose to check the *Not Needed* check box to display the link URL in the text instead.

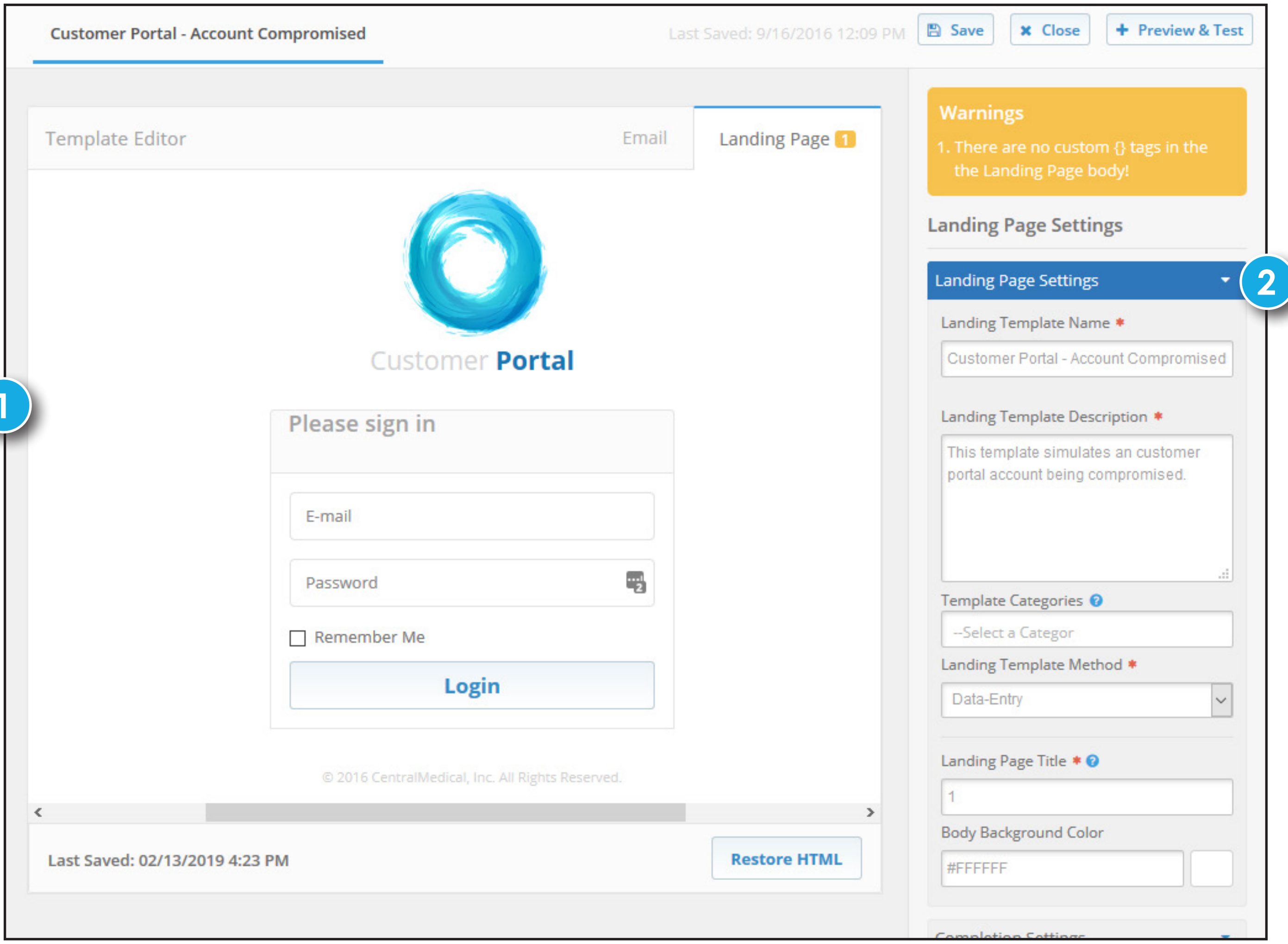
Custom Header Name & Value allow you to add your own custom header information to your email to help you whitelist and prevent test emails from going to the spam folder.

6 **Additional Links**

Edit HTML opens a pop up window where you can edit the email HTML directly.

Change Layout allows you to change the layout of the email.

Customizing Templates - Landing Page Tab



1 **Landing Page Editor** allows you to edit the content of the landing page through a WYSIWYG editor. Editable sections will be highlighted by a dashed orange box when you roll over them. A pop up window will open with the content.

2 **Landing Page Settings**

The Landing Template Name, Landing Template Description, and Template Categories work just as the email settings did.

Landing Template Method (previously Phishing Hook) is the type of simulation this template is replicating and tells the editor what fields are needed to customize the phishing experience on the landing page.

> **Data-Entry** is the most basic phishing method and will simply collect data from the targets using a form.
>
> **Download** will turn on additional fields to allow you to customize a file download.
>
> **URL-Replicate** allows you to replicate another website as your landing page. You will get an extra URL to Replicate field on the Template tab to enter the website you want to replicate. The Landing Page tab will also be locked out since the system will build it for you.

Landing Page Title is the text that will appear in the target's browser title.

Body Background Color allows you to change the background CSS color for the body tag.

Customizing Templates - Landing Page Tab

1 **Completion Settings** allows you to set up the next step in the phishing progression.

Completion Redirect Option allows you to select what will happen once a target completes the page action.

No Redirect means nothing will happen.

URL Redirect allows you to redirect the user to any URL you choose

Training Page allows you to select a training page to redirect the target to, either your own custom page or a system library page. There is also an option to copy the current training page (if one is already selected) and create a new page from scratch.

Completion Message is what will appear to the target in a javascript alert message when they complete the page action.

You also have the option to turn off tracking for completing the templates phishing hook action. This option is defaulted to *Yes*.

Download File Option

No File - Display Custom Message will only display the Completion Message

Download PDF with Message will allow the target to download a prebuilt PDF file and display the Completion Message.

Download EXE with Message will allow the target to download a prebuilt EXE file and display the Completion Message.

Download Custom File will provide additional fields to upload your own custom file.

2 **Misc. Settings**

From Submission Report Action allows you to customize how the system will display the action on the reports under the target's individual actions, such as if they fill out a form or download a file.

Use Bootstrap? allows you to use Bootstrap on the landing page. This option is defaulted to *Yes*.

3 **Additional Links**

Change Layout allows you to change the landing page layout.

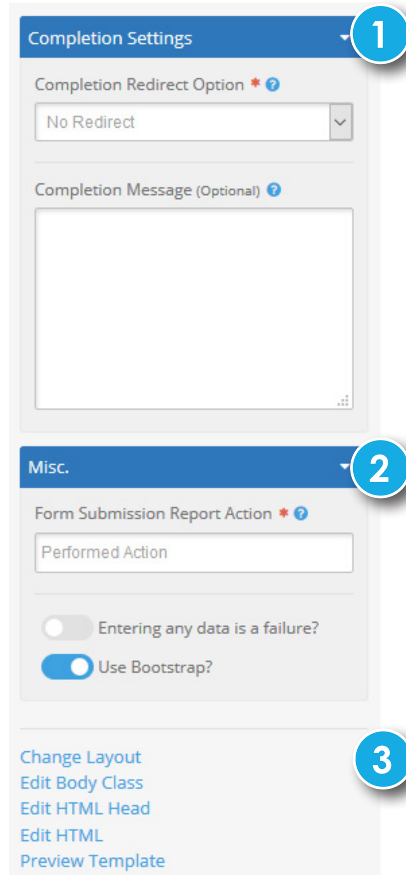
Edit HTML opens a pop up window allowing you to edit the landing page HTML directly.

The landing page automatically generates the <html>, <head>, <body>, and <form> tag for you. Everything you create will go inside the <form> tag. If you include these tags in your HTML it will cause errors on the landing page when loaded.

Edit Body Class opens a pop up window allowing you to enter the CSS body class you want to use.

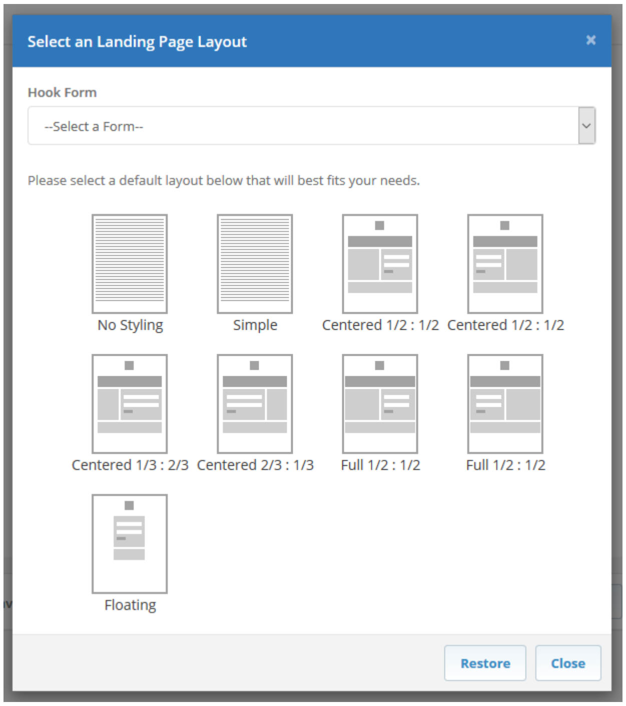
Edit HTML Head opens a pop up window allowing you to add content to the HTML head of the landing page.

Preview Template opens another tab with a preview of the landing page.



3 Additional Links

Change Layout allows you to change the landing page layout. A popup window will open and allow you to choose the Hook Form and the layout you wish to use. All of the current HTML and content on the landing page will be replaced. You can use the Restore button to undo your changes (before closing the window). There is also a Restore HTML button on the Landing Page Editor window that will restore the HTML to original condition (when the Landing Page was first loaded).



Edit Body Class opens a pop up window allowing you to enter the CSS body class you want to use.

Edit HTML Head opens a pop up window allowing you to add content to the HTML head of the landing page.

Edit HTML opens a pop up window allowing you to edit the landing page HTML directly.

Preview Template opens another tab with a preview of the landing page.

External Links

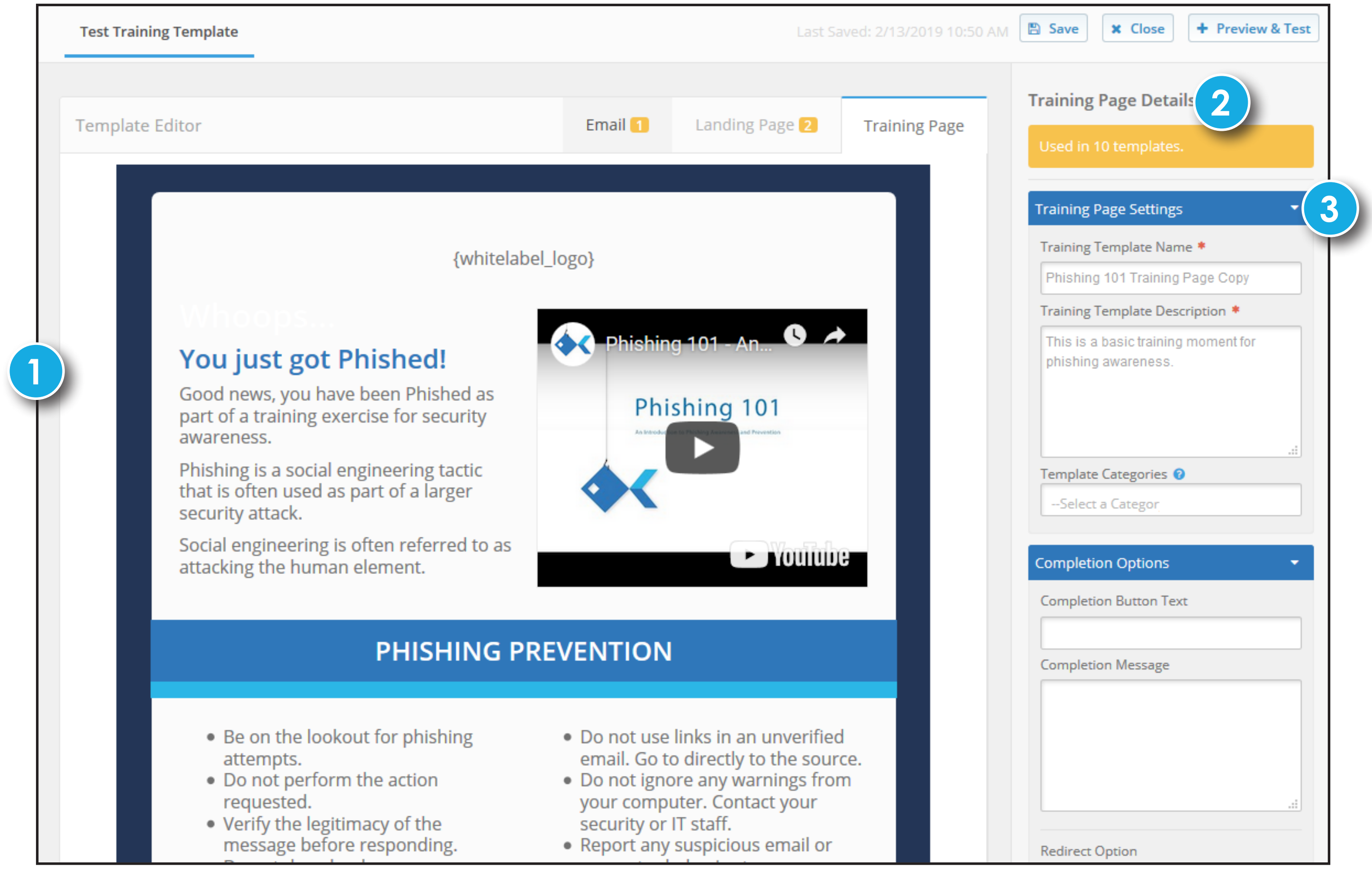
If you would like to add external links (that won't trigger the pages phishing hook) to your landing page you can add a class to your anchor tags.

Click Here

ignore-submit will bypass the page's default phishing hooks, but still record a failure. It will appear as "Clicked 3rd Party Link" in reporting.

training-link will bypass the page's default pishing hook and register as a training action. It will appear as "Clicked 3rd Party Training Link" in reporting.

Customizing Templates - Training Page Tab



1 **Training Page Editor** allows you to edit the content of the landing page through a WYSIWYG editor. Editable sections will be highlighted by a dashed orange box when you roll over them. A pop up window will open with the content.

2 **Template Connections Warning** lets you know how many other templates (both Email and Landing) this template is attached to. The Landing Page tab will also have this alert box. Given that Email, Landing, and Training templates are separate entities the same Training Template can be attached to multiple other Email and Landing Templates. This means, if you choose to edit the template you are affecting the phishing progression of all the other templates (including any active tests) that this template is attached to as well.

3 **Training Page Settings**

The Training Template Name, Training Template Description, and Template Categories work just as the email settings did.

Customizing Templates - Training Page Tab

4 **Completion Settings** allows you to set up the next step in the phishing progression.

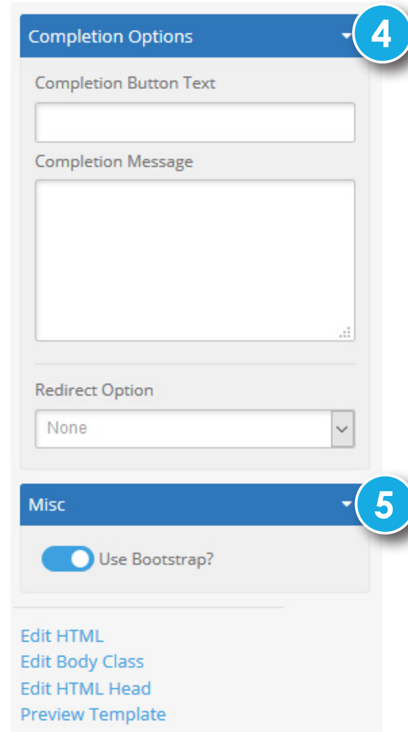
Completion Button Text is the text that appears in the "I have completed this training" button on the Training Page that the target uses to log that they have read the training provided. The default text is "Completed."

Completion Message is what will appear to the target in a javascript alert message when they complete the page action.

Completion Redirect Option allows you to select what will happen once a target completes the page action.

No Redirect means nothing will happen.

URL Redirect allows you to redirect the user to any URL you choose.



5 **Additional Links**

Edit HTML opens a pop up window allowing you to edit the landing page HTML directly.

Edit Body Class opens a pop up window allowing you to enter the CSS body class you want to use.

Edit HTML Head opens a pop up window allowing you to add content to the HTML head of the landing page.

Preview Template opens another tab with a preview of the landing page.

Template Editor - Available Variables

Variable	Description
{hook_url}	Displays the configured URL and unique tracking code of the hook. This tag also used when making an image clickable.
{hook_link}	Displays the anchor text configured for the hook URL.
{phish_key}	
{fname}	Displays the first name of the target
{lname}	Displays the last name of the target
{email}	Displays the email address of the target
{group_name}	Displays the group name of which the target is a member
{sub_group_name}	Displays the sub group name that the target is assigned
{to_1}	Displays the Optional Field 1 of the target
{to_2}	Displays the Optional Field 2 of the target
{to_3}	Displays the Optional Field 3 of the target
{go_1}	Displays the Optional Field 1 assigned to the group
{go_2}	Displays the Optional Field 2 assigned to the group
{go_3}	Displays the Optional Field 3 assigned to the group
{ip_address}	Displays the IP Address from where the target is coming from. NOTE: can only be used on landing pages. Do not use in emails.
{date}	Displays the current date
{datetime}	Displays the current date and time
{company}	Displays the target's company name
{title}	Displays the target's title
{address_one}	Displays the target's address line 1
{address_two}	Displays the target's address line 2
{city}	Display's the target's city
{state}	Display's the target's state
{zip}	Display's the target's postal code
{country}	Display's the target's country
{phone_business}	Display's the target's business phone number
{phone_business_fax}	Display's the target's business fax number
{phone_mobile}	Display's the target's mobile phone number

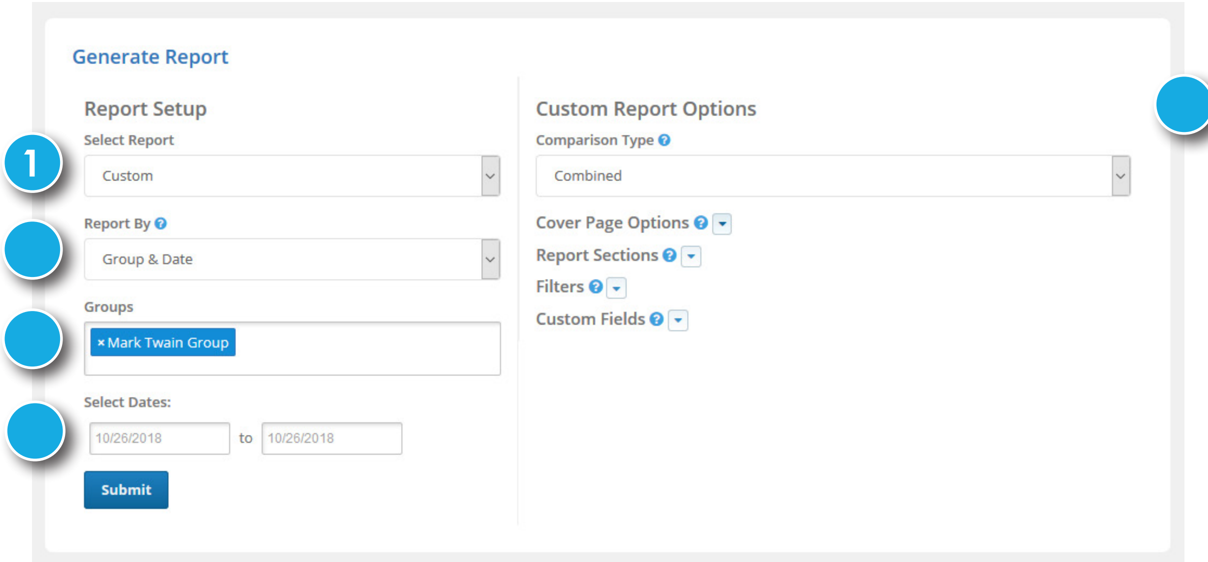
If the group or target variables are changed before or during another test, changes will reflect in all tests. That is, the target and group variables are not tied to the test, but to the target or group.

Examples of use of optional fields:

Optional Group fields: These three fields could be used to identity common information across an organization that could be used during a test, such as the organization's regulator or audit company.

Optional Target Fields: These three fields could be used to identify specific information related to that target, such as the target's supervisor, office location, etc.

Reporting



Select Report

Pick the report you want to generate. You can choose from one of our pre-defined reports or create a completely custom report of your own.

There are several report types available.

Full Report: All activity for a specific report listed.
Failed Only: List only targets that failed a test.
Summary-By Date: List the results for a given group for a given time period.
Summary-By Test: List the results for given test(s).
Comparison-By Date: List the results and changes between two different time periods for a given group.
Comparison-By Test: List the results and changes between two different tests.
Repeat Failures-By Date: List only targets that have failed more than once in a given time period.
Repeat Failures-By Test: List only targets that have failed more than once on a given test.
Individual Target: List all actions by one target on all tests involved.
Custom: Allows you to select which reporting section you want to include on your report.

"Report By" Option

Select how you wish to pull your data.

Group, Group & Date, Test, Test & Date, Individual, Individual & Date

Depending on what you select for "Report By," you will either get a multi-select dropdown to choose on which groups, tests, or individual targets you want to run a report.

Select Dates

If you choose one of the options involving date selection you will get input fields to choose dates.

Custom Report Option

Items 1 through 4 are the only required fields if you are using one of the pre-defined reports. The following sections are for customized reporting.

Comparison Type is how you would like to display certain charts on the report.

Combined will display the pie charts as a single combined data chart.

Comparison will display a pie chart for each test in the pulled data.

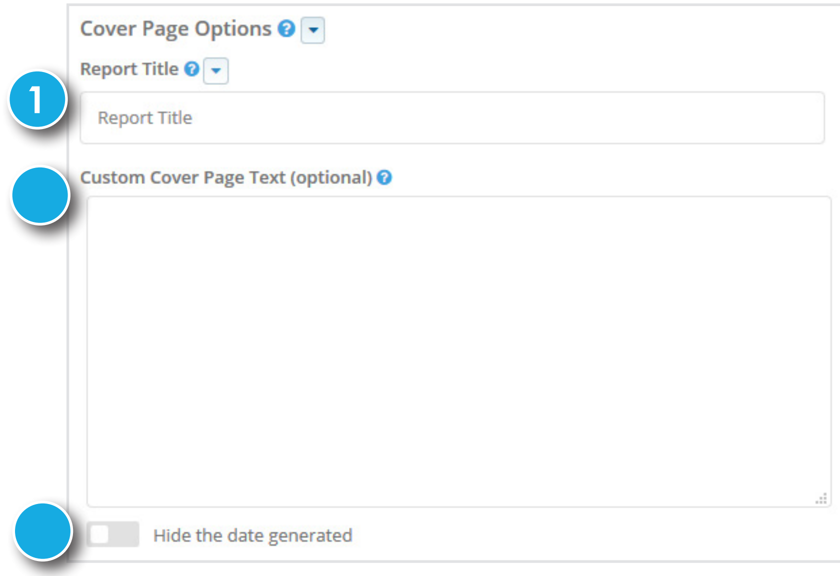
Both will display both a combined and individual chart for each test.

The sections listed below are covered on the following pages.

Cover Page Options
Report Sections
Filters
Custom Fields

Cover Page Options

These options allow you to make changes to the PDF cover page when you generate the report.



1 Report Title

The **report title** is generated by default based upon the report type and data. However, if you wish to enter your own title you can do so here. This title will appear on the cover page and file name.

Custom Cover Page Text

This is custom text that will appear on the cover page of your report when it is generated as a PDF. You can use paragraph, break, bold, and italic html tags. All other tags will be stripped.

Hide the date generated

By default, the date and time the report is generated will appear on the cover page of the PDF. However, if you wish to hide this date check this box.

Reporting

Report Sections

Test Summary gives the overall stats (counts for targets, messages, passed, failed, unique counts, and averages) for all the tests in the data pulled. This chart combines all tests in the data pulled as one set of statistics. This section pairs well with the Average Pass/Fail Pie Chart.

Passed vs. Failed Pie Chart shows the percentages of targets who passed and failed for the tests in the pulled data.

Most Severe Action by Target Pie Chart shows count/percentages for the most severe (worst) action that each user committed during the test(s). Each target is only counted once per test in this pie chart.

Average Pass/Fail Pie Chart shows the average count/percentage of passess and fails for all the tests in the pulled data.

Failure Activity Breakdown Pie Chart shows all the failure activity for all the tests in the data pulled. This chart combines all the tests in the pulled data as one set of statistics. Every action committed by the targets is included in this data (i.e., targets can be counted more than once).

Test Comparison By Dates compares two date periods for messages sent, targets passed, targets failed, and the difference between the two date ranges for each. This chart can only be accessed when using the Comparison-By Date report.

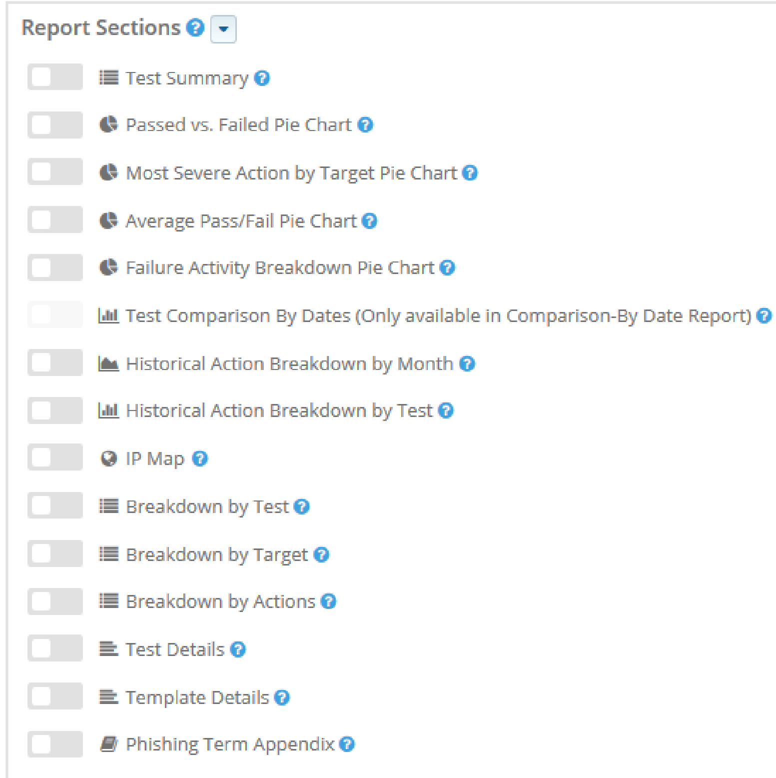
Historical Actions Breakdown by Month area chart shows the delivered, opened, clicked, data extended, and received training categories over the given date range of the data pulled.

Historical Action Breakdown by Test bar chart shows the delivered, opened, clicked, data extended, and received training categories for all the tests included in the data pulled.

IP Map plots the IP addresses of the actions on a world map so that you can see where the traffic is coming from.

Breakdown by Test shows the data at the test level.

Breakdown by Target shows the data at the target level. Each individual test will be listed under the target.

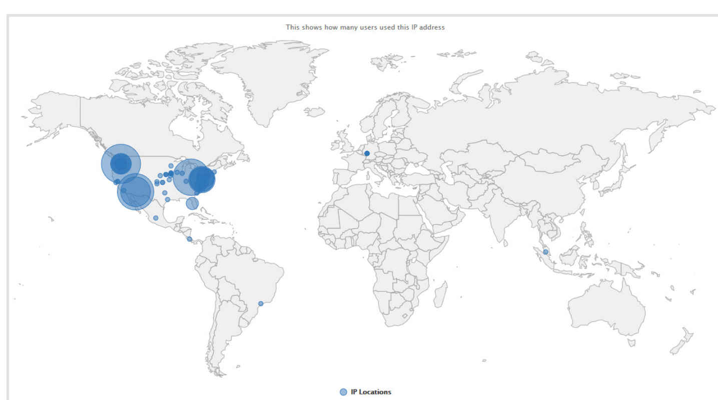


Breakdown by Actions shows the data at the action level. Data will include action time, the time it took for the action to occur (i.e., Phish Time), action type, IP address, browser, OS, and template.

Test Details will show the set up information for each test in the pulled data.

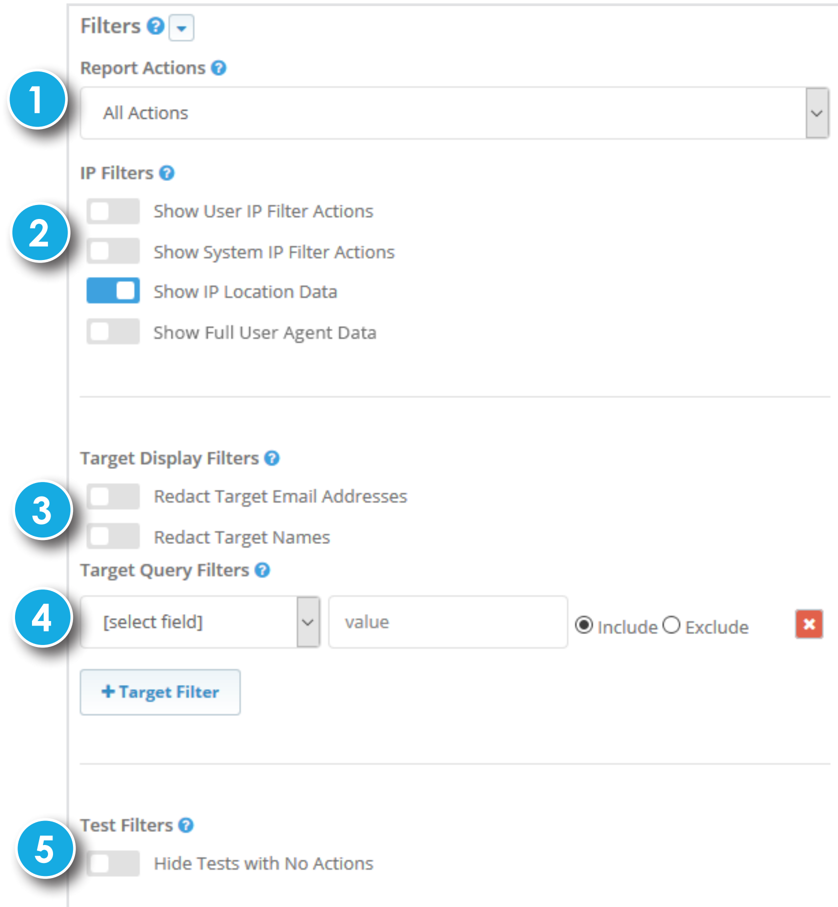
Template Detials shows the set up information for each template used in the pulled data.

Phishing Term Appendix lists any phishing specific terms that may be usedul for interrepting the data.



Filters

These options all you to filter the pulled data according to your needs.



1 Report Actions

Allows you to choose what actions will be reported. You can choose to have **All Actions** included, **Failed Only** actions, or **Repeat Fails Only**.

2 IP Filters

Show User IP Filter Actions allows you to display the actions filtered out by the IPs listed on the Testing Defaults page. Displaying these actions does not cause them to be counted.

Show System IP Filter Actions allows you to display the actions filtered out by the known security software IP addresses that the system automatically filters out for you. *Displaying these actions does not cause them to be counted.*

Show IP Location Data allows you to turn on/off the coordinate data of the IP addresses.

Show Full User Agent Data allows you to turn on/off the full user agent string for the user's actions.

3 Target Display Filters

Redact Target Email Addresses allows you to hide the email addresses of your targets in the report. For security reason, this is advised for sending via email.

Redact Target Names allows you to hide the names of your targets in the report. For security reason, this is advised for sending via email.

4

Target Query Filters allow you to customize the data pulling queries to include/exclude matching your criteria. You can choose from any of the pre-defined target fields and any custom fields you have created.

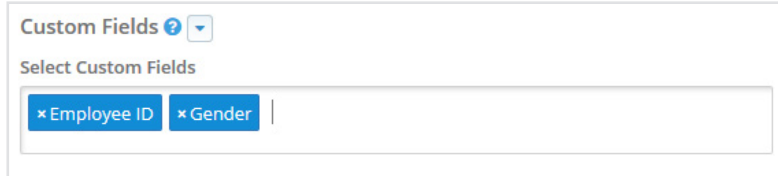
5 Test Filters

Hide Test with No Actions allows you to hide tests that have no actions from displayed data. This only effects the data displayed, not the analysis data.

Reporting

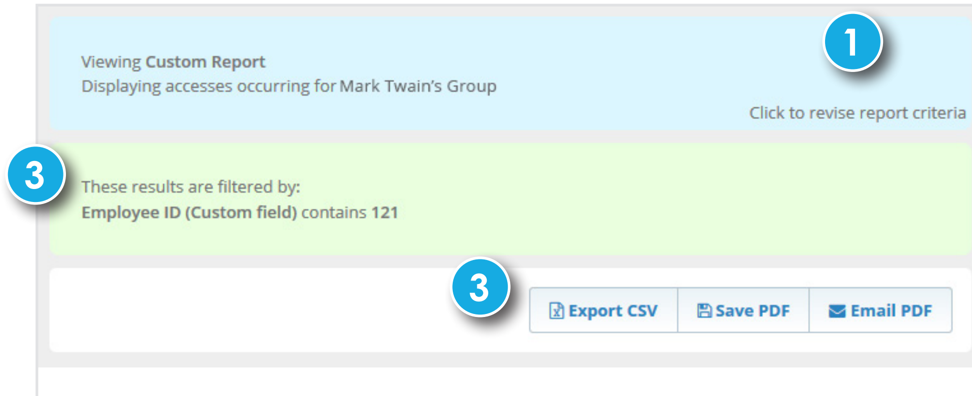
Custom Fields

This dropdown allows you to add any of your custom field data to the target rows in the report. For spacing reasons, it is advised to not add more than 5 fields.



Post Report Generation Options

Once your report has been generated the top of the screen will contain some basic data for your review.



1 Report and Revision Options

The blue area gives basic information about the type of report you generated and a link to re-open and revise the form creation criteria.

2 Filters

The green area will display he filtering options you set up.

3 Saving Your Data

There are three options for retrieving the report from the system.

Export CSV will print the report data (minus a few section like the IP Map data) into CSV format. This allows you to upload or manipulate the data as you see fit.

Save PDF will save the report as a PDF for you to download or view in your browser.

Email PDF allows you send the report to anyone you want directly from the system.