

---

# GRAPHUS

## MSP Settings

### Feature Guide

---



## MSP Settings

---

Go to

1. [Overview](#)
2. [What Do Save as Default, Apply or Save as Default and Apply Buttons Mean?](#)
3. [MSP Branding](#)
4. [Whitelisting](#)
5. [EmployeeShield® Application on Suspicious and Not Yet Trusted Senders](#)

---

### 1. Overview

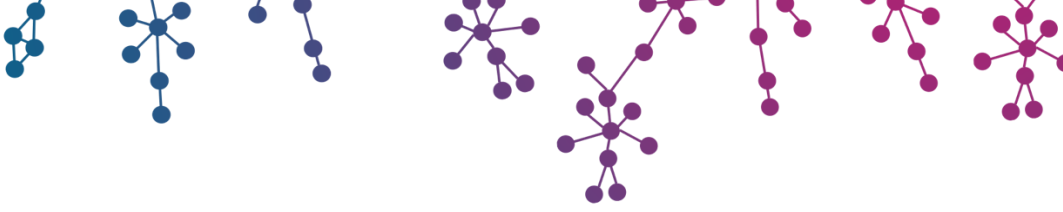
The MSP Settings page hosts settings of various types that can be managed and configured for MSP end customers (organizations) from a central location. This reduces the overhead of MSP admin to configure different settings for each of their organizations individually. MSPs have the flexibility to configure these settings to their own liking and apply them to either all their organizations or to a subset of their organizations with just a few clicks.

This page offers the following capabilities:

1. MSPs can apply their own brand to Graphus customer facing reports and EmployeeShield® (warning banner on emails).
2. MSPs can whitelist their trusted domains, mail-from domains and IP addresses so that Graphus does not flag emails having these attributes. It helps with false positives reduction.
3. MSPs can also choose to apply or not apply EmployeeShield® to emails received from un-trusted senders. These are additional EmployeeShield® application that MSPs have an option to enable aside from the Quarantine and various other types of EmployeeShield® capabilities that Graphus offers by default.

### 2. What Do – , , and Buttons Mean?

Every section present on MSP Settings page has three common buttons. The first is **Save as Default**, the second is **Apply**, and the third is **Save as Default and Apply**.



### MSP Settings

[User Guide](#)

**Branding**

Reports Branding

On Customize Daily Insights and Monthly Reports

Logo  No file chosen Logo Preview

Logo will be applied to all reports.  
Acceptable image types are jpg, jpeg and png.  
Acceptable resolution is within the range of 400 x 200 pixels.

Header and Footer Color

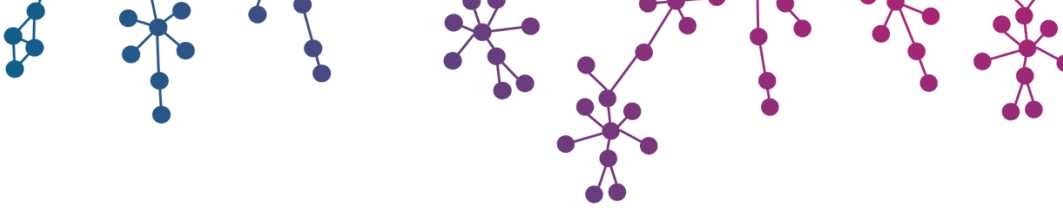
Color will be applied to report header and footer.

These buttons work in the following way:

1. **Save as Default:** This will save the default settings at MSP level, which will be applied to organization which MSP will onboard in future. These settings will not be applied to existing organizations until they click on the Apply button and select organizations to propagate these settings.
2. **Apply:** This button is independent of the **Save as Default** button. It will selectively apply or propagate settings to single or multiple organizations without making any changes in default settings.
3. **Save as Default and Apply:** This button gives you the combined capability of the **Save as Default** and **Apply** buttons. It will save the default settings at MSP level along with the option to apply or propagate the selected features to single or multiple organizations. Any future organizations onboarding on the Graphus platform will inherit these settings by default.

Here are some example scenarios on the usage of these buttons:

1. **Scenario 1: Existing Graphus MSP, protecting organizations and configuring settings for the first time.** You have two options.
  - a. **First option:** Configure the settings and save them as default by clicking **Save as Default**. This will save the settings BUT will not apply them to any of your existing organizations. You can come back to the settings page at a later time and apply these settings to your existing organizations by clicking the Apply button. You will have the option of choosing a subset or all of your organizations. **Save as Default** will, however,

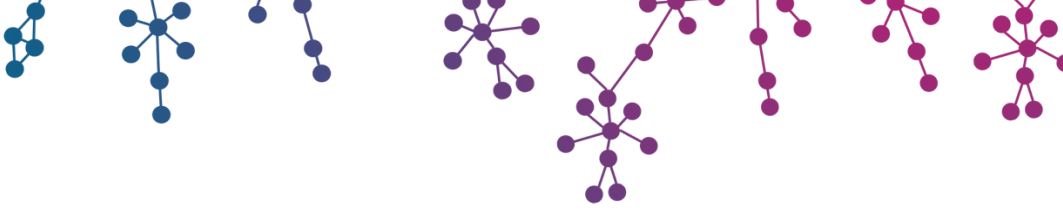


- apply these settings automatically to any new organizations onboarding on Graphus in future.
- b. **Second option:** Configure the settings, save them as default and also apply them to your organizations by clicking **Save as Default and Apply**. You will have the option of choosing a subset or all of your organizations. These settings will also automatically apply to any new organization onboarding on Graphus in future.
2. **Scenario 2: New Graphus MSP with no organizations under protection and configuring settings for the first time.** You can only save the settings by clicking **Save as Default**. Since you have no organizations under protection so far, the Apply button is irrelevant. **Save as Default** will, however, apply these settings automatically to any new organizations onboarding on Graphus in future.
  3. **Scenario 3: Existing Graphus MSP protecting organizations, already configured settings in the past and making changes now.** You have two options:
    - a. **First option:** After changes are made, you can save the settings by clicking **Save as Default**. The modified settings will NOT apply to any of your existing organizations, they will continue to use the old settings. You can come back to the settings page at a later time and apply the modified settings to your existing organizations by clicking on the Apply button. **Save as Default** will, however, apply the modified settings automatically to any new organizations onboarding on Graphus in future.
    - b. **Second option:** After changes are made, you can save them as defaults and also apply them to your organizations by clicking **Save as Default and Apply**. You will have the option of choosing a subset or all of your organizations. The modified settings will also apply to any new organization onboarding on Graphus in future.

The following sections cover the various settings available on the MSP Settings page.

### 3. MSP Branding

The MSP Branding section is where you can apply your own brand (logo and colors) to Graphus daily and monthly reports and EmployeeShield®. If MSPs do not want to use their own brand they can continue to use the default Graphus logo and colors.



### MSP Settings

[User Guide](#)

#### Branding

##### Reports Branding

On Customize Daily Insights and Monthly Reports

Logo  No file chosen Logo Preview

Logo will be applied to all reports.  
Acceptable image types are jpg, jpeg and png.  
Acceptable resolution is within the range of 400 x 200 pixels.

Header and Footer Color

Color will be applied to report header and footer.

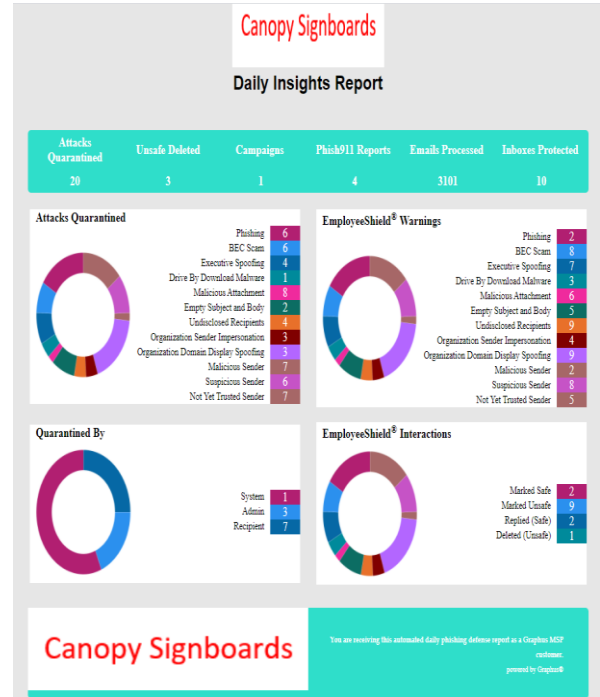
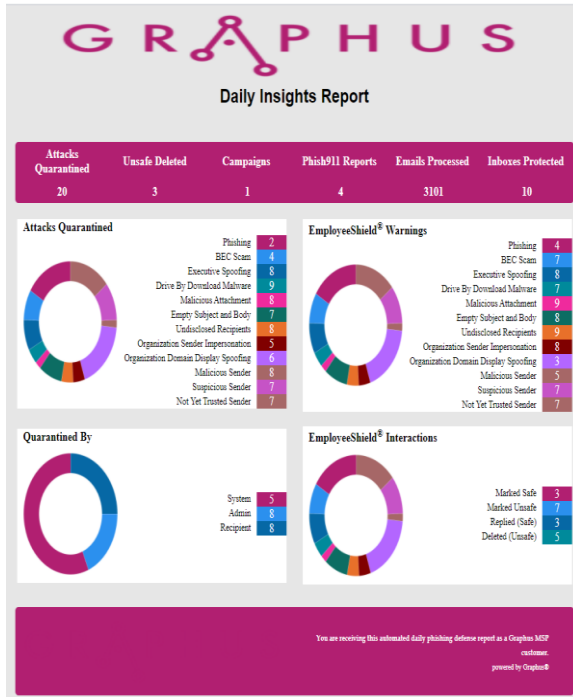
**Report Customization:** This allows you to customize the Graphus daily and monthly reports with your logo and a color for the header and footer. MSPs can preview the report in HTML or PDF format using the respective buttons.

1. Make sure the  On button is turned on. By default, the button is turned off. The Graphus provided default logo and color will show up when the button is toggled ON for the first time.
2. **Logo:** Click **Choose File** and upload your logo. The image file should be in jpg, jpeg, png or gif format. Make sure the resolution of the image is within 400 x 200. As soon you upload the logo, you will be able to see a preview of the logo on to the right side.
3. **Header and Footer Color:** Click inside the text box for the color palette to appear. Select a color of your choice by dragging the dot inside the square to a specific location. Also, you can drag the slider bar up or down to move between hues of different colors. Alternatively, you can manually enter the color code.
4. Click **Done**. The selected color's code appears in the textbox.



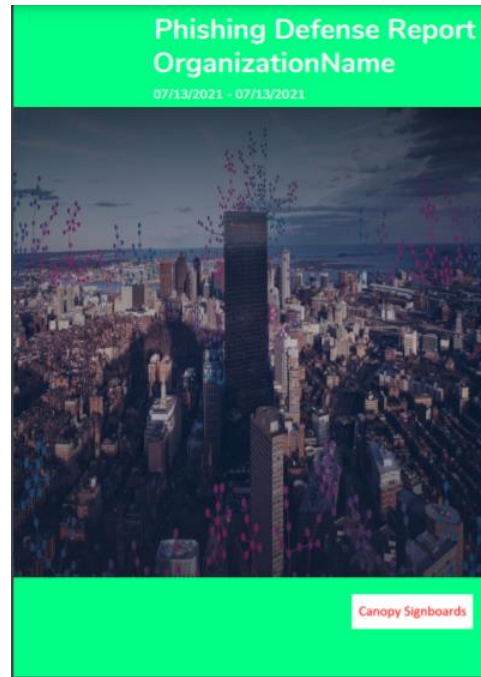
**Preview HTML Report**

5. **Preview HTML Report**: Click this button to preview the report in HTML format. This template will then be applied to the Daily Insights Report and Monthly Report, and this is how the reports will look like to your customers when they receive them. Samples of both default report and custom report are given below.





6. **Preview PDF Report**: Click this button to preview the report in PDF format. This is how the PDF Report will look like to your customers when they receive it. Samples of both default report and custom report are given below.



**Phishing Defense Report - Graphus**  
07/01/2021 - 07/31/2021

**EXECUTIVE SUMMARY**  
For the time period 07/01/2021 - 07/31/2021 a total of 17,268 emails were analyzed post-delivery for your organization. Using the best-in-class detection and prevention methodology, 2 attacks were detected to be quarantined, 15 suspicious emails were detected and EmployeeShield® (Interactive warning banner) applied. During the same period, no suspicious emails were reported by the end users. These sophisticated attacks were missed by all other email security controls deployed by your organization, but detected and remediated by Graphus.

	<b>INBOXES PROTECTED</b>	21
	<b>EMAILS PROCESSED</b>	17,268
	<b>UNSAFE DELETED</b>	0
	<b>CAMPAIGNS</b>	0
	<b>PHISH911</b>	0
	<b>ATTACKS QUARANTINED</b>	2

**ATTACKS QUARANTINED SUMMARY**

	<b>PHISHING / SPEAR PHISHING</b>	2
	<b>BEC SCAMS</b>	2
	<b>IDENTITY SPOOFING</b>	0
	• Executive Spoofing	0
	• Organization Sender Impersonation	0
	<b>MALWARE / RANSOMWARE</b>	0
	• Drive-by	0
	• Attachment	0

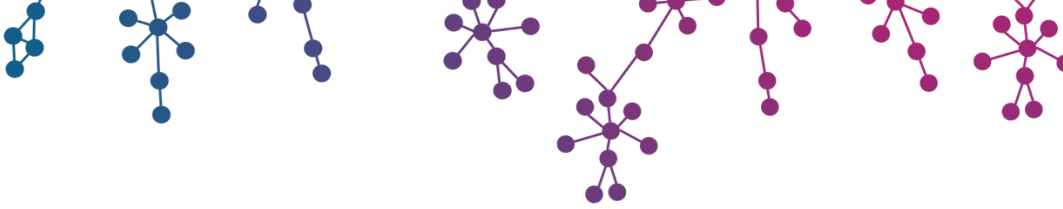
**Phishing Defense Report - OrganizationName**  
07/13/2021 - 07/13/2021

**EXECUTIVE SUMMARY**  
For the time period 07/13/2021 - 07/13/2021 a total of 501 emails were analyzed post-delivery for your organization. No attacks were detected to be quarantined. No suspicious emails were detected. During the same period, no suspicious emails were reported by the end users.

	<b>INBOXES PROTECTED</b>	11
	<b>EMAILS PROCESSED</b>	501
	<b>UNSAFE DELETED</b>	0
	<b>CAMPAIGNS</b>	0
	<b>PHISH911</b>	0
	<b>ATTACKS QUARANTINED</b>	0

**ATTACKS QUARANTINED SUMMARY**

	<b>PHISHING / SPEAR PHISHING</b>	0
	<b>BEC SCAMS</b>	0
	<b>IDENTITY SPOOFING</b>	0
	• Executive Spoofing	0
	• Organization Sender Impersonation	0
	<b>MALWARE / RANSOMWARE</b>	0
	• Drive-by	0
	• Attachment	0



7. Click **Save as Default**, **Apply** or **Save as Default and Apply** as the case may be.

**EmployeeShield® Branding:** In this section, you can customize the EmployeeShield® or warning banner look and feel.

### EmployeeShield® Branding

**On** Email recipients in your organization will see EmployeeShield® (interactive warning banner) inserted at the top of suspicious emails. It will have detailed message explaining why the email has been classified as suspicious. Recipient will be able to mark the email as safe or unsafe. The exact look and feel of EmployeeShield® can be configured below.

**Interactivity**

Make EmployeeShield® interactive, links to report email as Phishing (Unsafe) or False Positive (Safe) will be available to email recipients. (Recommended).

Keep EmployeeShield® informational only, there will not be any interactive links available to email recipients.

**Logo Text**  Organization name to show at the top left of EmployeeShield®.

**Background Color**  **Message Color**

**Safe Link Color**  **Unsafe Link Color**

**Safe Link Label**  **Unsafe Link Label**

**Message**

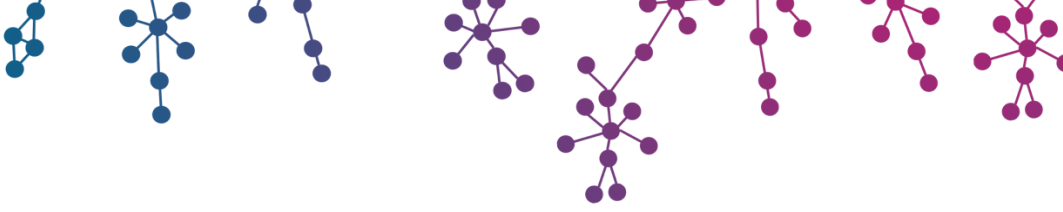
Use Graphus generated detailed messages. These messages will change depending on the type of phishing detection. (Recommended).

Provide your own message. This will be a static message and will not change depending on the type of phishing detection.

**Rollout**  By Default EmployeeShield® will be enabled for all protected accounts. Organization specific rollout of limited users can be done at organization level settings page.

1. Make sure the  **On** button is turned on. The Graphus provided default values will show up when the button is toggled ON for the first time.
2. **Interactivity:** By default, the second radio button is selected. If you keep this selected, the banner will have only information to communicate but no links to take action from the recipient's side. If you select the first radio button, the banner will appear with interactive links (to mark the sender as Safe and Unsafe). This option is recommended by Graphus.
3. **Logo Text:** This is the organization name that will show on the top left corner of the EmployeeShield®. MSPs can provide their own name in this box if they prefer.
4. **Background Color:** Click inside the text box for the color palette to appear, and select a color of your choice by dragging the dot inside the square to a specific location.
5. **Message Color:** You can select a color for your message. Select a color of your choice from the palette.
6. **Safe Link Color:** You can select a color for safe link.
7. **Unsafe Link Color:** You can select a color for unsafe link.





8. **Safe Link Label:** This is the name to be provided for the safe link. For example, *Safe*. You can use any custom word to denote the same meaning. This is the link that the recipient has to click if they wish to mark the email as false positive.
9. **Unsafe Link Label:** This is the name to be provided for the unsafe link. For example, *Unsafe*. You can use any custom word to denote the same meaning. This is the link that the recipient has to click if they wish to mark the email as a phishing attack.
10. **Message:** By default, the first radio button is selected. Graphus recommends this selection. The messages under this option will change depending on the type of phishing detection. Select the second radio button if you want to provide a static custom message of your own. This message will not change depending on the type of phishing detection. You can preview this custom message by clicking the **Preview Sample** button.
11. **Rollout:** By default, the EmployeeShield® will be rolled out for all protected accounts. You can enable EmployeeShield® for selected users for an organization from the Settings page for that specific organization.
12. Click **Save as Default**, **Apply** or **Save as Default and Apply** as the case may be.

## Setup Flow Example:

**Option 1:** If you click **Save as Default**, you will see the following screen.

### EmployeeShield® Branding



EmployeeShield® default settings saved successfully. Applied changes may take up to 24 hours to reflect.

On

Email recipients in your organization will see EmployeeShield® (interactive warning banner) inserted at the top of suspicious emails. It will have detailed message explaining why the email has been classified as suspicious. Recipient will be able to mark the email as safe or unsafe. The exact look and feel of EmployeeShield® can be configured below.

Interactivity  Make EmployeeShield® interactive, links to report email as Phishing (Unsafe) or False Positive (Safe) will be available to email recipients. (Recommended).  
 Keep EmployeeShield® informational only, there will not be any interactive links available to email recipients.

Logo Text  Organization name to show at the top left of EmployeeShield®.

Background Color  Message Color

Safe Link Color  Unsafe Link Color

Safe Link Label  Unsafe Link Label

Message  Use Graphus generated detailed messages. These messages will change depending on the type of phishing detection. (Recommended).  
 Provide your own message. This will be a static message and will not change depending on the type of phishing detection.

Preview Sample

Cancel Changes

Rollout  By Default EmployeeShield® will be enabled for all protected accounts. Organization specific rollout of limited users can be done at organization level settings page.

Save as Default

Apply

Save as Default and Apply



**Option 2 and 3:** If you click **Apply** or **Save as Default and Apply**, you will see the following screen.

### Organizations Settings Application

#### Modified Settings

Email recipients in your organization will see EmployeeShield® inserted at the top of suspicious emails	ON
Background Color	#ffbb00
Message Color	#ffffff
Organization name to show at the top left of EmployeeShield®	Canopy Signboards Inc
Safe Link Color	#ffffff
Safe Link Label	Safe
Unsafe Link Color	#ffffff
Unsafe Link Label	Unsafe
Adds links to report email as Phishing (Unsafe) or False Positive (Safe).	ON
Rollout for all users (EmployeeShield® will now be applied to all protected accounts. Any previous rollout related settings will be overridden. Please go to the organization settings page to make changes related to rollout.)	ON

---

#### Apply Modified Settings to Selected Organizations

Please select organizations below to modify the settings.

<input type="button" value="Select"/>	testdomain1175.com	<input type="button" value="Select"/>	testdomain1176.com
<input type="button" value="Select"/>	testdomain1177.com	<input type="button" value="Select"/>	testdomain1178.com

---



You can click **Select All** to apply the settings to all the organizations listed below or you can click **Deselect All** to deselect all the organizations listed there. Alternatively, you can select the **Select/Deselect** button next to each organization to select or deselect the organization. Once you have done your selections, click **Next**. You will see the following confirmation screen.

### Organizations Settings Application Confirmation

Following action will be taken on the organizations listed below.

**EmployeeShield® changes to be applied**

Email recipients in your organization will see EmployeeShield® inserted at the top of suspicious emails	ON
Background Color	#ffbb00
Message Color	#ffffff
Organization name to show at the top left of EmployeeShield®	Canopy Signboards Inc
Safe Link Color	#ffffff
Safe Link Label	Safe
Unsafe Link Color	#ffffff
Unsafe Link Label	Unsafe
Adds links to report email as Phishing (Unsafe) or False Positive (Safe).	ON
Rollout for all users (EmployeeShield® will now be applied to all protected accounts. Any previous rollout related settings will be overridden. Please go to the organization settings page to make changes related to rollout.)	ON

---

Organizations list:

testdomain1175.com	testdomain1176.com
testdomain1177.com	testdomain1178.com

---

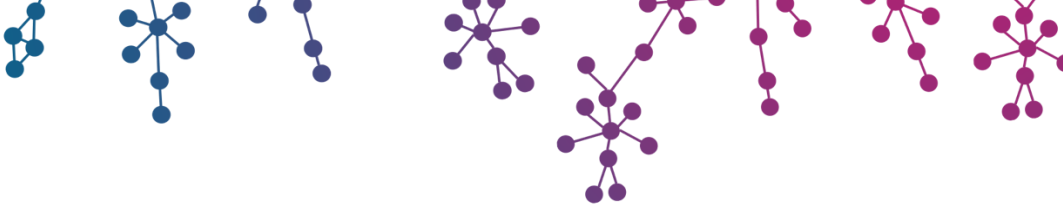
Review the settings being applied and click **Confirm**. You will see the following message.

Successfully applied organizations settings.

[MSP Settings](#)

## 4. Whitelisting

Graphus will skip processing any inbound email with attributes that match the whitelisted parameters. This means that no Quarantine or EmployeeShield® functionalities in Graphus will be applied to such emails. There are three different types of whitelisting capabilities provided on the platform.



1. **Whitelist Sender Domain:** Skip processing inbound emails whose sender email address has the configured domain.
2. **Whitelist SMTP Mail From Domain:** Skip processing inbound emails whose smtp.mailfrom domain and the SPF value match with the configured values.
3. **Whitelist IP Address:** Skip processing inbound emails whose smtp.mailfrom server IP Address match with the configured values.

When you come to the whitelisting section, none of the radio buttons will be selected.

### Whitelisting

Whitelist Sender Domain  Whitelist SMTP Mail From Domain  Whitelist IP Address

View Default

Save as Default

Apply

Save as Default and Apply

Select one of the three options from the section. Irrespective of what option you select, you can click the View Default button and see the current default settings.

### Current Default Whitelisting

Sender Domains	
<input type="button" value="Keep"/>	testdomain1175.com
<input type="button" value="Keep"/>	testdomain1177.com

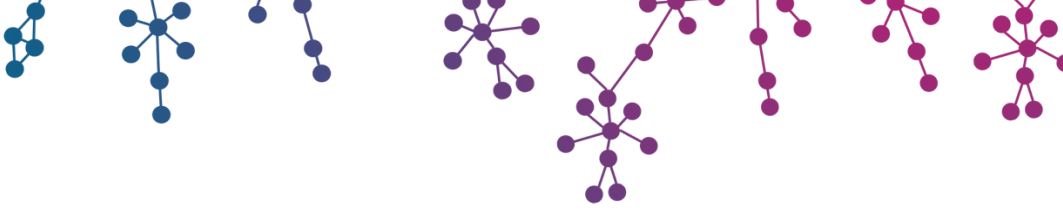
---

SMTP Mail From Domains	SPF Value	
<input type="button" value="Keep"/>	testdomain1176.com	pass
<input type="button" value="Keep"/>	testdomain1177.com	pass

---

IP Address	
<input type="button" value="Keep"/>	14.14.14.14

You also have the option to remove any of the defaults here.



Toggle the **Keep/Remove** button next to the domain, SMTP mail from domain or IP address to remove that value. You will see **Remove Default**, **Apply**, and **Remove Default and Apply** buttons as shown below.

### Current Default Whitelisting

Sender Domains	
<input type="checkbox"/> Keep	testdomain1175.com
<input checked="" type="checkbox"/> Remove	testdomain1177.com

---

SMTP Mail From Domains	SPF Value	
<input type="checkbox"/> Keep	testdomain1176.com	pass
<input type="checkbox"/> Keep	testdomain1177.com	pass

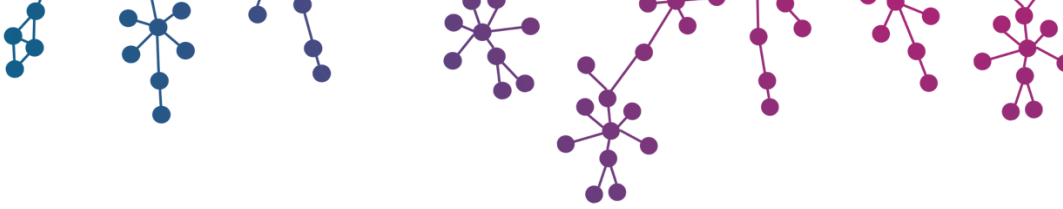
---

IP Address	
<input type="checkbox"/> Keep	14.14.14.14

**Option 1:** If you click **Remove Default**, you will see the following screen.

Successfully updated Whitelisting.

[MSP Settings](#)



**Option 2:** If you click **Apply** or **Remove Default and Apply**, you will see the following screen.

### Organizations Settings Application

Modified Settings  
Whitelistsings will be removed  
testdomain1177.com

---

Apply Modified Settings to Selected Organizations Select All Deselect All

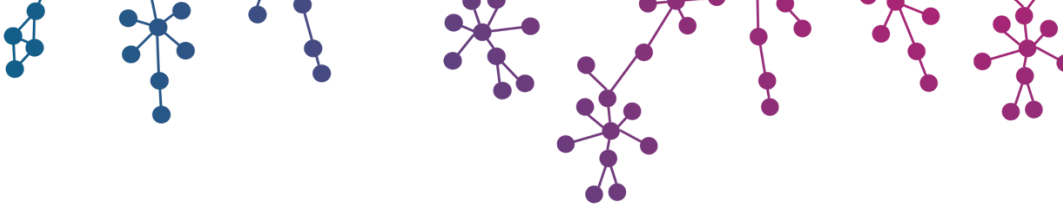
Please select organizations below to modify the settings.

<input type="checkbox"/>	testdomain1175.com	<input type="checkbox"/>	testdomain1176.com
<input type="checkbox"/>	testdomain1177.com	<input type="checkbox"/>	testdomain1178.com

---

Next Cancel

You can click **Select All** to apply the settings to all the organizations listed below or you can click **Deselect All** to deselect all the organizations listed there. Alternatively, you can select the **Select/Deselect** button next to each organization to select or deselect the organization. Once you have done your selections, click **Next**. You will see the following screen.



## Organizations Settings Application Confirmation

Following action will be taken on the organizations listed below.

Whitelisting will be removed

Sender Domains:

testdomain1177.com

Organizations list:

testdomain1175.com

testdomain1176.com

testdomain1177.com

testdomain1178.com

Confirm

Cancel

Click **Confirm**. You will see the following message.

Successfully applied organizations settings.

[MSP Settings](#)

If you already have default settings and want to apply them to certain organizations, you can do so by clicking the **Apply** button. You will see the following screen.

## Organizations Settings Application

Modified Settings

Default whitelisting will be added  
testdomain1177.com

Apply Modified Settings to Selected Organizations

Select All

Deselect All

Please select organizations below to modify the settings.

Select

testdomain1175.com

Select

testdomain1176.com

Select

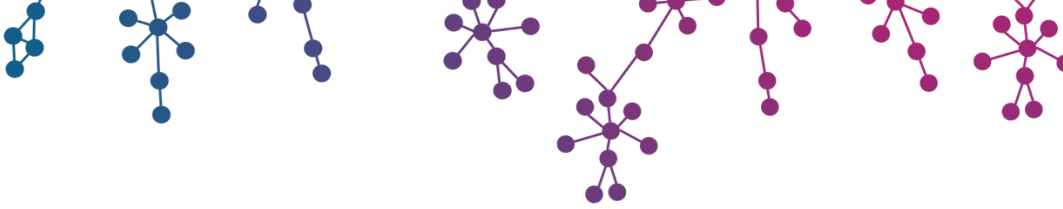
testdomain1177.com

Select

testdomain1178.com

Next

Cancel



You can click **Select All** to apply the settings to all the organizations listed below or you can click **Deselect All** to deselect all the organizations listed there. Alternatively, you can select the **Select/Deselect** button next to each organization to select or deselect the organization. Once you have done your selections, click **Next**. You will see the following screen.

### Organizations Settings Application Confirmation

Following action will be taken on the organizations listed below.

Whitelisting will be added

Sender Domain:  
testdomain1177.com

---

Organizations list:

testdomain1175.com	testdomain1176.com
testdomain1177.com	testdomain1178.com

---

Review the settings being applied and click **Confirm**. You will see the following confirmation message.

Successfully applied organizations settings.

[MSP Settings](#)

### Setup Flow Example:

You can select one of the below radio buttons and click **Save as Default**, **Apply** or **Save as Default and Apply**.

If you want to select **Whitelist Sender Domain**, do the following:

1. Select the **Whitelist Sender Domain** radio button.
2. Enter the domain in the textbox.
3. Click **Add Row** to add more text boxes or click **Remove Row** to remove extra boxes.
4. Click **Save as Default**, **Apply** or **Save as Default and Apply** as the case may be.





### Whitelisting

Whitelist Sender Domain  Whitelist SMTP Mail From Domain  Whitelist IP Address

Add Row Remove Row

testdomain1177.com

View Default Save as Default Apply Save as Default and Apply

If you want to select **Whitelist SMTP Mail From Domain**, do the following:

1. Select the **Whitelist SMTP Mail From Domain** radio button.
2. Enter the domain in the textbox. Select an SPF value from the dropdown.
3. Click **Add Row** to add more text boxes or click **Remove Row** to remove extra boxes. Select an SPF value from the dropdown for each domain that you add.
4. Click **Save as Default**, **Apply** or **Save as Default and Apply** as the case may be.

### Whitelisting

Whitelist Sender Domain  Whitelist SMTP Mail From Domain  Whitelist IP Address

Add Row Remove Row

testdomain1176.com

pass

View Default Save as Default Apply Save as Default and Apply

If you want to select **Whitelist IP Address**, do the following:

1. Select the **Whitelist IP Address** radio button.
2. Enter the IP address in the textbox. The IP address has to be in the x.x.x.x format.
3. Click **Add Row** to add more text boxes or click **Remove Row** to remove extra boxes.
4. Click **Save as Default**, **Apply** or **Save as Default and Apply** as the case may be.

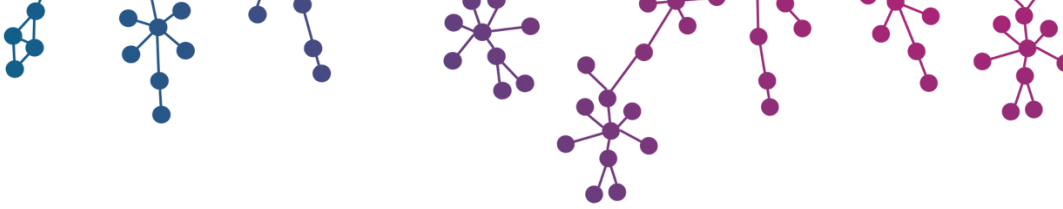
### Whitelisting

Whitelist Sender Domain  Whitelist SMTP Mail From Domain  Whitelist IP Address

Add Row Remove Row

14.14.14.14

View Default Save as Default Apply Save as Default and Apply



**Option 1:** If you select any of the three options (i.e. **Whitelist Sender Domain**, **Whitelist SMTP Mail From Domain** or **Whitelist IP Address**) and click **Save as Default**.

1. Select any of the three options.
2. Enter the domain name in xxxxxx.xxx format for the first two options. Enter the IP address in x.x.x.x. format for the third option.
3. Click the **Save as Default** button. You will see the following screen.

#### Whitelisting

 Successfully added whitelisting. Click on 'View Default' to check current values. Applied changes may take up to 24 hours to reflect.

Whitelist Sender Domain  Whitelist SMTP Mail From Domain  Whitelist IP Address

View Default

Save as Default

Apply

Save as Default and Apply

**Option 2 and 3:** If you select any of the three options (i.e. **Whitelist Sender Domain**, **Whitelist SMTP Mail From Domain** or **Whitelist IP Address**) and click **Apply** or **Save as Default and Apply**.

Select any of the three options, enter the domain names or IP addresses, and click **Apply** or **Save as Default and Apply**. You will see the following screen.

### Organizations Settings Application

#### Modified Settings

##### Whitelisted SMTP Mail From Domain

Domain  
testdomain1177.com

SPF Value  
pass

#### Apply Modified Settings to Selected Organizations

Select All

Deselect All

Please select organizations below to modify the settings.

Select

testdomain1175.com

Select

testdomain1176.com

Select

testdomain1177.com

Select

testdomain1178.com

Next

Cancel



*Note: For the Whitelist Sender Domain and Whitelist IP Address options, you will not find the SPF value on the top right. Other things remain the same.*

You can click **Select All** to apply the settings to all the organizations listed below or you can click **Deselect All** to deselect all the organizations listed there. Alternatively, you can select the **Select/Deselect** button next to each organization to select or deselect the organization. Once you have done your selections, click **Next**. You will see the following screen.

### Organizations Settings Application Confirmation

Following action will be taken on the organizations listed below.

Whitelisting will be added

SMTP Mail From Domain:

Domain	SPF Value
testdomain1177.com	pass

---

Organizations list:

testdomain1175.com	testdomain1176.com
testdomain1177.com	testdomain1178.com

---

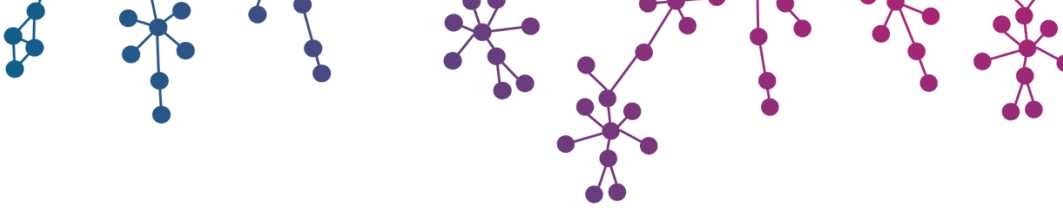
Click **Confirm**. You will see the following message.

Successfully applied organizations settings.

[MSP Settings](#)

## 5. EmployeeShield® Application on Suspicious and Not Yet Trusted Senders

MSPs have the option to enable additional types of EmployeeShield® to be applied on suspicious emails received from untrusted senders. This is in addition to the Quarantine and several other types of EmployeeShield® that Graphus applies by default.



Turning this setting ON will apply EmployeeShield® on an email that is received from either a completely new external sender or from a sender who is not a trusted sender yet in the TrustGraph. There are additional settings that can be turned ON in this section to control this at a finer level by choosing the second and third options.

#### EmployeeShield® Application on Suspicious and Not Yet Trusted Senders

Suspicious and Not Yet Trusted are senders who have not established a Trusted trust rating in the Trust Graph for the organization. Example: First time senders. Graphus will apply EmployeeShield® on emails received from such senders based on the settings below.

- Off Apply EmployeeShield® when an email is received from a Suspicious or a Not Yet Trusted Sender.
- On Apply EmployeeShield® when an email with attachments and links is received from a Suspicious or a Not Yet Trusted Sender.
- On Apply EmployeeShield® when an email with authentication failures (SPF/DKIM/DMARC) is received from a Suspicious or a Not Yet Trusted Sender.

Save as Default

Apply

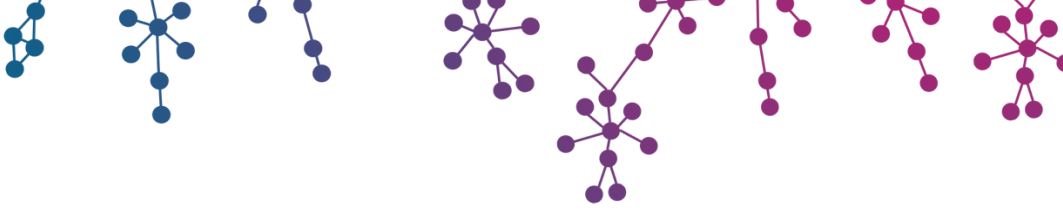
Save as Default and Apply

These settings can be enabled or disabled in three different ways:


1. **Apply EmployeeShield® when an email is received from a Suspicious or a Not Yet Trusted Sender:** Graphus will apply EmployeeShield® on an email received from such senders. If you enable this setting, then the other two settings are covered by default.
2. **Apply EmployeeShield® when an email with attachments and links is received from a Suspicious or a Not Yet Trusted Sender:** Graphus will apply EmployeeShield® on an email with attachments and links received from such senders.
3. **Apply EmployeeShield® when an email with authentication failures (SPF/DKIM/DMARC) is received from a Suspicious or a Not Yet Trusted Sender:** Graphus will apply EmployeeShield® on an email with either SPF, DKIM or DMARC authentication failures received from such senders.

#### Setup Flow Example:

**Option 1:** If you switch on the first button or the other two buttons and click **Save as Default**, you will see the following screen.



### EmployeeShield® Application on Suspicious and Not Yet Trusted Senders

 Successfully saved default values. Applied changes may take up to 24 hours to reflect.

Suspicious and Not Yet Trusted are senders who have not established a Trusted trust rating in the Trust Graph for the organization. Example: First time senders. Graphus will apply EmployeeShield® on emails received from such senders based on the settings below.

- Off Apply EmployeeShield® when an email is received from a Suspicious or a Not Yet Trusted Sender.
- On Apply EmployeeShield® when an email with attachments and links is received from a Suspicious or a Not Yet Trusted Sender.
- On Apply EmployeeShield® when an email with authentication failures (SPF/DKIM/DMARC) is received from a Suspicious or a Not Yet Trusted Sender.

**Option 2:** If you switch on the first button or the other two buttons and click **Apply** or **Save as Default and Apply**, you will see the following screen.

### Organizations Settings Application

#### Modified Settings

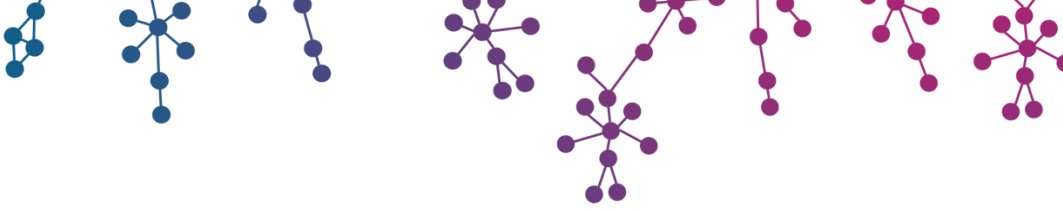
Apply EmployeeShield® when an email is received from a Suspicious or a Not Yet Trusted Sender.	OFF
Apply EmployeeShield® when an email with attachments and links is received from a Suspicious or a Not Yet Trusted Sender.	ON
Apply EmployeeShield® when an email with authentication failures (SPF/DKIM/DMARC) is received from a Suspicious or a Not Yet Trusted Sender.	ON

#### Apply Modified Settings to Selected Organizations

Please select organizations below to modify the settings.

- |                                       |                    |                                       |                    |
|---------------------------------------|--------------------|---------------------------------------|--------------------|
| <input type="button" value="Select"/> | testdomain1175.com | <input type="button" value="Select"/> | testdomain1176.com |
| <input type="button" value="Select"/> | testdomain1177.com | <input type="button" value="Select"/> | testdomain1178.com |

You can click **Select All** to apply the settings to all the organizations listed below or you can click **Deselect All** to deselect all the organizations listed there. Alternatively, you can select the **Select/Deselect** button next to each organization to select or deselect the organization. Once you have done your selections, click **Next**. You will see the following screen.



## Organizations Settings Application Confirmation

Following action will be taken on the organizations listed below.

Apply EmployeeShield® when an email is received from a Suspicious or a Not Yet Trusted Sender.	OFF
Apply EmployeeShield® when an email with attachments and links is received from a Suspicious or a Not Yet Trusted Sender.	ON
Apply EmployeeShield® when an email with authentication failures (SPF/DKIM/DMARC) is received from a Suspicious or a Not Yet Trusted Sender.	ON

### Organizations list:

testdomain1175.com	testdomain1176.com
testdomain1177.com	testdomain1178.com

Confirm

Cancel

Click **Confirm**. You will see the following message.

Successfully applied organizations settings.

[MSP Settings](#)

## © Copyright

All rights reserved. No part of this document may be reprinted or reproduced or utilized in any form or by any electronic, mechanical or other means, now known or hereinafter invented, including photocopying and recording or in any information storage or retrieval system without written permission from the publishers.