

# Proofpoint Settings Overview

## Contents

How to get support .....	1
Login to Portal** .....	2
Search for Quarantined Messages** .....	3
Emergency Inbox.....	4
Spam Settings.....	5
Digests.....	6
Sender Lists** .....	7
Quarantine Report** .....	8

Note: \*\* indicates the most important functions of the system.

## How to get support

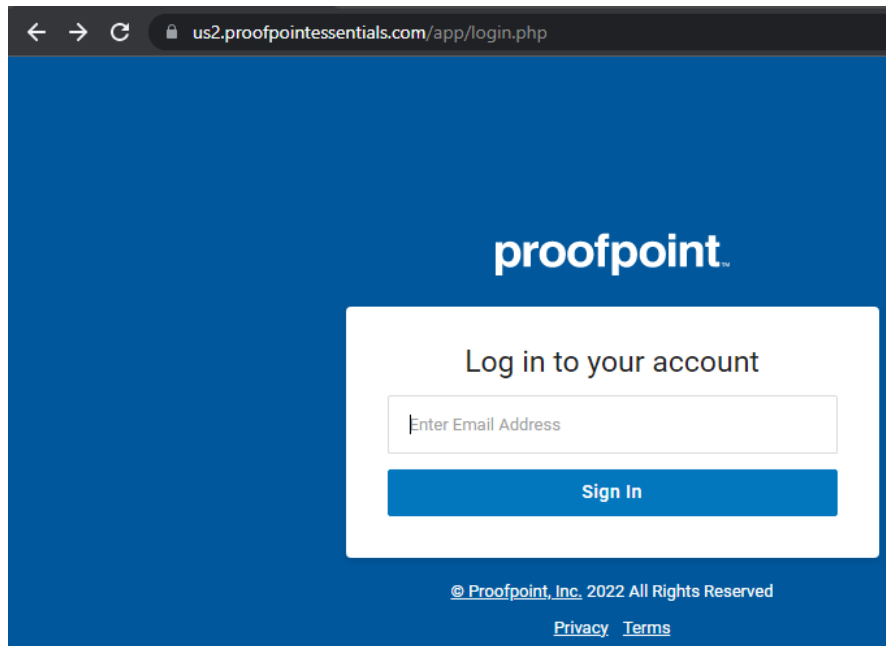
Call: **470-481-0400** option **2**

E-Mail: [support@cengatech.com](mailto:support@cengatech.com)

Browse: <https://support.cengatech.com>

We are available 8am – 5pm Monday through Friday for standard support and 24/7 for Emergency support through the phone system only.

## Login to Portal\*\*

A screenshot of a web browser showing the login page for Proofpoint. The browser's address bar displays "us2.proofpointessentials.com/app/login.php". The page has a dark blue background with the "proofpoint." logo in white. In the center, there is a white box containing the text "Log in to your account", a text input field with the placeholder "Enter Email Address", and a blue "Sign In" button. At the bottom of the page, there is a copyright notice: "© Proofpoint, Inc. 2022 All Rights Reserved" and two links: "Privacy" and "Terms".

us2.proofpointessentials.com/app/login.php

proofpoint.

Log in to your account

Enter Email Address

Sign In

© Proofpoint, Inc. 2022 All Rights Reserved

[Privacy](#) [Terms](#)

Browse to <https://us2.proofpointessentials.com>

Login with your email address and email password. If prompted select Sign in with Microsoft.

## Search for Quarantined Messages\*\*

The screenshot shows the 'Tim Brogdon Email Log' interface. On the left is a navigation sidebar with options like 'Log Search', 'Emergency Inbox', 'Administration', 'Profile', 'Aliases', 'Spam Settings', 'Digests', 'Groups', and 'Allow/Block Sender Lists'. The main area has search filters: 'Type' (Inbound mail), 'Status' (Quarantined), and 'Date/Time' (2022/09/16 0:00 - 2022/09/22 23:59). Below the filters are 'SEARCH', 'CLEAR', and 'ADVANCED SEARCH' buttons. A table of messages is displayed with columns: To, Subject, Date/Time, Classification, Threat Type, Threat Level, Size, Status, and Actions. The 'Actions' column has a dropdown menu open, showing options like 'Release from quarantine', 'Release and approve', 'Resend', 'Classify as spam', 'Classify as clean', 'Hide email from logs', and 'Hemper <contact@hemper.co>'. The table lists several messages, including one from 'Hemper <contact@hemper.co>' and another from 'xfinity@emails.xfinity.com'.

To	Subject	Date/Time	Classification	Threat Type	Threat Level	Size	Status	Actions
tim@brogdon.net	12 Months of Gaming + a Lifetime of C...	2022/09/22, 07:09	Spam	Spam	🟡🟡🟡	93.9 kB	Quarantined	👁️ ⋮
tim@brogdon.net	Not sure where to start? 🤔	2022/09/22, 00:21	Spam	Spam	🟡🟡🟡	136.4 kB	Quarantined	👁️ ⋮
tim@brogdon.net	^I noticed my co-worker spraying pain...	2022/09/21, 23:45	Fraud	DMARC	🔴🔴🔴	68.8 kB	Quarantined	👁️ ⋮
tim@brogdon.net	Blue Sona and Litra Beam: Your new st...	2022/09/21, 18:35	Spam	Spam	🟡🟡🟡	107.4 kB	Quarantined	👁️ ⋮
tim@brogdon.net	\$15 for Unlimited Xbox Gaming 🎮	2022/09/21, 17:10	Spam	Spam	🟡🟡🟡	66.9 kB	Quarantined	👁️ ⋮
tim@brogdon.net	Equipment upgrades every three years ...	2022/09/21, 16:13	Spam	Spam	🟡🟡🟡	109.3 kB	Quarantined	👁️ ⋮

Click on Log Search

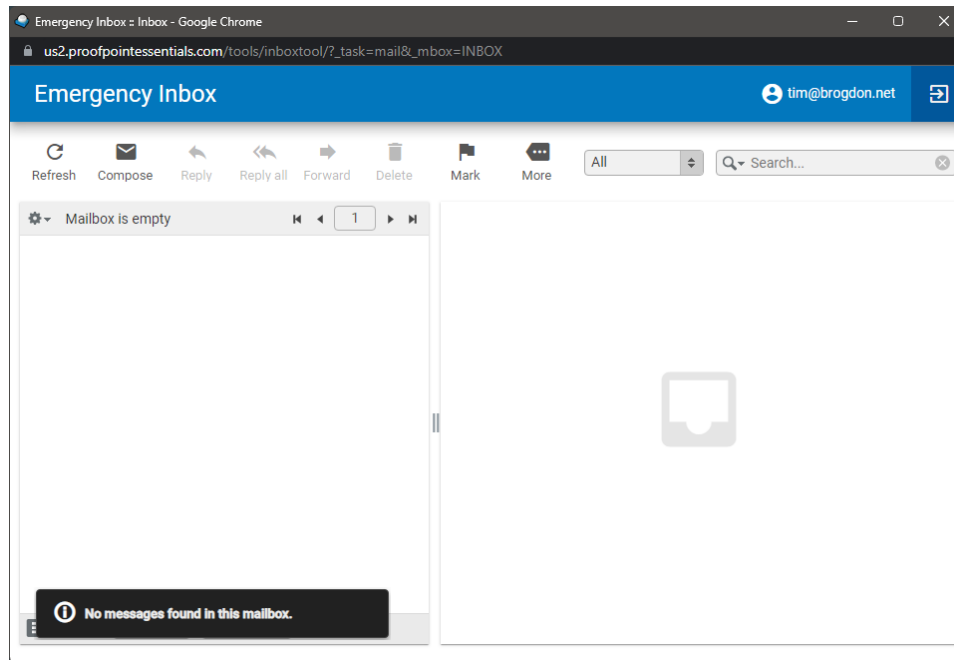
Select the filters you want to search on or just click search to use the defaults

Locate the message you want to release and check the box next to it.

Use the drop down box called Actions

Select Release and Approve to always allow the sender through

## Emergency Inbox



In the event your Office 365 email service is unavailable, you can use the Emergency Inbox to send and receive emails until Office 365 service returns to normal. This is a basic system that will only show emails received since the service went down.

## Spam Settings

Spam Settings

Spam Sensitivity

Current Trigger Level 7

Adjust how sensitive our spam engine will treat suspicious email. The lower the number the more sensitive.

Quarantine bulk email

Yes

Place any email suspected as bulk in the quarantine.

Spam stamp & forward

No

Add a tag to the subject of any email that may be spam that our engine was unsure about.

Spam stamp & forward subject tag

\*\*\*Spam\*\*\*

Customise the tag that will appear in the subject line of a spam stamp and forwarded email.

Include an easy-spam-reporting disclaimer in passed email

Yes

This will add a disclaimer to emails stating that they have been scanned for spam and virus. It also includes an option for reporting misclassifications.

Backscatter prevention

Yes

SAVE

© Proofpoint, Inc. 2004-2022 All Rights Reserved - Version 5.20220914

Here you can adjust the Spam Filtering for your specific account. Changes here will not affect other users. We set industry standard settings for all users, but you may change this to fit your specific needs.

### *Spam Sensitivity*

The default is 7, moving this to a larger number will make the detection less sensitive and a smaller number more sensitive.

### *Quarantine bulk email*

This tries to detect newsletters and like email that may be bothersome but not a security risk.

### *Spam stamp & forward*

This will add **\*\*\*Spam\*\*\*** to any message that looks like spam but does not meet all criteria. This can help still get emails to your inbox but warn you with the subject line adjustment so you can review the message further.

### *Include an easy-spam-reporting disclaimer in passed email*

This adds a section at the bottom of all emails received with a link to report the message as spam to Proofpoint. Using this can help Proofpoint to better detect email as spam in the future.

### *Backscatter prevention*

This is recommended to remain on. This is mail system messages that can be used by hackers to learn more about your email setup. Blocking these can help prevent this activity and better protect the mail system.

## Digests

**Tools**

- Log Search
- Emergency Inbox

**Administration**

- Profile
- Aliases
- Spam Settings
- Digests**
- Groups
- Allow/Block Sender Lists

### Digests

Enable digests for user  
Yes

Only include messages quarantined since the last Quarantine Digest was sent  
Yes

Quarantine digests will only include message that have been quarantined after the last digest was sent.

Quarantine Digest delivery start time  
07:00  
The time the digest will be sent to your users.

Interval between digest checks  
24 h  
Interval between quarantine digest checks

Retention period  
30 days  
How far back you want the digest to cover.

Timestamp of last Quarantine Digest check  
**07:00:01 EDT, Thursday 22 September 2022**

---

Include emails that have been quarantined by:

- Organization filters and/or blocked sender list entries
- Group filters and/or blocked sender list entries
- End-user filters and/or blocked sender list entries

---

Exclude messages from the Quarantine Digest that are most likely to be spam  
Exclude messages from the digest that score very high for spam.

**SAVE**   SEND DIGEST   PREVIEW DIGEST

Here you can setup when you get the spam quarantine report as well as set advanced settings on how the report functions. By default, this will send in the morning.

You can change the Interval between digest checks to get the quarantine report more frequently. For example, you could set this to 12 hours to get a report in the morning and at night.

## Sender Lists\*\*

The screenshot shows the 'Sender Lists' configuration page. On the left is a dark sidebar with navigation options: 'Tools' (Log Search, Emergency Inbox), 'Administration' (Profile, Aliases, Spam Settings, Digests, Groups), and 'Allow/Block Sender Lists'. The main content area is titled 'Sender Lists' and contains two sections:

- Blocked Sender List:** A text input field with the placeholder 'Enter your Blocked sender list separated by line, comma or semi-colon...'. Below it, text states: 'Messages from addresses, domains or IP addresses that you include on the blocked sender list will be quarantined.' Instructions follow: 'To add addresses, domains (e.g., \*@domain.com, \*@\*.domain.com) or IP addresses to the list, type them in the text box and use a line, comma or semi-colon to separate entries. IP addresses may contain wildcards (e.g., 10.20.\*.20, 10.\*.\*, 10.\*.0.\*) and CIDR notation (e.g., 10.0.62.0/24). Click the save button to save your changes.'
- Safe Sender List:** A scrollable list of email addresses: '0101016b6aed7ce5-d93b5a77-f2f0-48f5-a5af-c7f1d3ab23ac-000000@us-west-2.amazonaws.com', '01010175db786cd4-6547ffe1-4c7c-4f2a-a3f2-6795ff799871-000000@us-west-2.amazonaws.com', '112-hil-492.0.153448.0.0.5671.9.765546@em-sj-77.mktomail.com', and '1800ushanks@notifications.usbank.com'. Below it, text states: 'Messages from addresses, domains or IP addresses that you include on the safe sender list will not be quarantined.' Instructions follow: 'To add addresses, domains (e.g., \*@domain.com, \*@\*.domain.com) or IP addresses to the list, type them in the text box and use a line, comma or semi-colon to separate entries. IP addresses may contain wildcards (e.g., 10.20.\*.20, 10.\*.\*, 10.\*.0.\*) and CIDR notation (e.g., 10.0.62.0/24). Click the save button to save your changes.'

A blue 'SAVE' button is located at the bottom of the main content area.

Here is where you can manually input senders you want to always block or never block. You can enter the full email address or domain name. I.e. [tim@cengatech.com](mailto:tim@cengatech.com) or Cengatech.com. You cannot enter your own domain name, since this is a way for hackers to work around the blocking.

### *Blocked Sender List*

Enter any email address or domain name you want to always go to the Quarantine Box

### *Safe Sender List*

Enter any email address or domain name you want to always allow.

The only exception to this is any email detected to have a virus attachment or fails all checks. Those messages will still be Quarantined and may need our assistance to release.

# Quarantine Report\*\*

The screenshot shows an email titled "Proofpoint Essentials - Quarantine Digest" from "Secure Email <do-not-reply@proofpointessentials.com>" to "Sales Department". It includes a "Quarantine Digest" header with a "Sign in to your account" link and a date/time stamp of "2022-09-20 08:00 EDT". Below this is a table with columns for "Address", "Subject", "Delivery Date/Time", and "Action". One entry is visible for "Vivek Puri" with the subject "Your learning content" and delivery time "20 Sep 22 - 07:36 AM". The "Action" column for this entry lists "Preview", "Release", "Release & Approve", and "Block". At the bottom, there are links for "Sign in to your account" and "Request new digest", along with a copyright notice for Proofpoint, Inc. 2004-2022.

Address	Subject	Delivery Date/Time	Action
Vivek Puri bounce+ccc2bf78fcc-sales=cengatech.com@mail.tabletwise.com	Your learning content	20 Sep 22 - 07:36 AM	Preview Release Release & Approve Block

This is the email report you receive once a day in the morning. Through this report you have a few functions you can do without accessing the portal...

Next to each email you will see Actions, here you can perform actions on the specific email that was blocked.

*Preview* – This gives you a safe web based preview of the email, recommended if you do not recognize the sender. This will not load any images or attachments.

*Release* – This will release this one message and take no other action, wait a minutes or two and you should receive the email in your inbox as normal.

*Release & Approve* – If you know the sender is safe, select this option to release the message and add the sender to the whitelist (safe sender list).

*Block* – If you know the message is spam, use this to alert Proofpoint that the message was properly marked as spam. This can help future detection, but is safe to ignore as well.

NOTE: At any time, you may return to this quarantine report and click on **Request new digest**, at the bottom of the quarantine list, this will email you a new quarantine report containing all emails since your last report. This allows you to see any blocked messages without accessing the online portal.