YSU Tech Desk
...a division of Media & Academic Computing
Hours:
Monday and Friday 7:30 am - 5:00 pm
Tues, Wed, and Thurs 7:30 am - 8:00 pm
Saturday 9:00 am - 5:00 pm
Phone: (330)941-1595 e-Mail: techdesk@cc.ysu.edu
http://techdesk.ysu.edu

YSU Spam Solution Guide to Using Proofpoint

Proofpoint Web Interface

Introduction

In 2006, YSU deployed the Proofpoint appliance in response to a growing number of spam messages infiltrating their way past current detection technologies into user's mailboxes. In January 2013, the University chose to move to a cloud-based implementation of Proofpoint and limit filtering to YSU email addresses ending in @ysu.edu that belong to Faculty and Staff members.

How It Works

The Proofpoint appliance acts as a mail proxy, filtering mail and passing what it believes are legitimate messages to the user's inbox. This filtering only applies on YSU mail accounts with addresses ending in @ysu.edu. The system uses a very detailed set of algorithms to accurately determine spam from legitimate mail. This means fewer false-positives and more protection for your mailbox. However, if you do not wish to have your mail filtered for spam or are comfortable with your desktop client filtering software, please see the **Using the Proofpoint interface - Profile** section at the end of this document.

The Proofpoint appliance also provides encrypted email functionality. This is triggered by adding [secure] or [encrypt] anywhere in the subject line.

What Do I Have To Do?

On a weekly basis, users will receive an End User Digest in their inbox. From the digest, users can delete, release, or mark messages as "Not Junk" that were filtered and identified by Proofpoint. All filtered mail will reside on the Proofpoint appliance **for 21 days** until the messages are deleted or released manually to the user's inbox. After 21 days, the mail flagged as spam **will be eliminated** automatically.

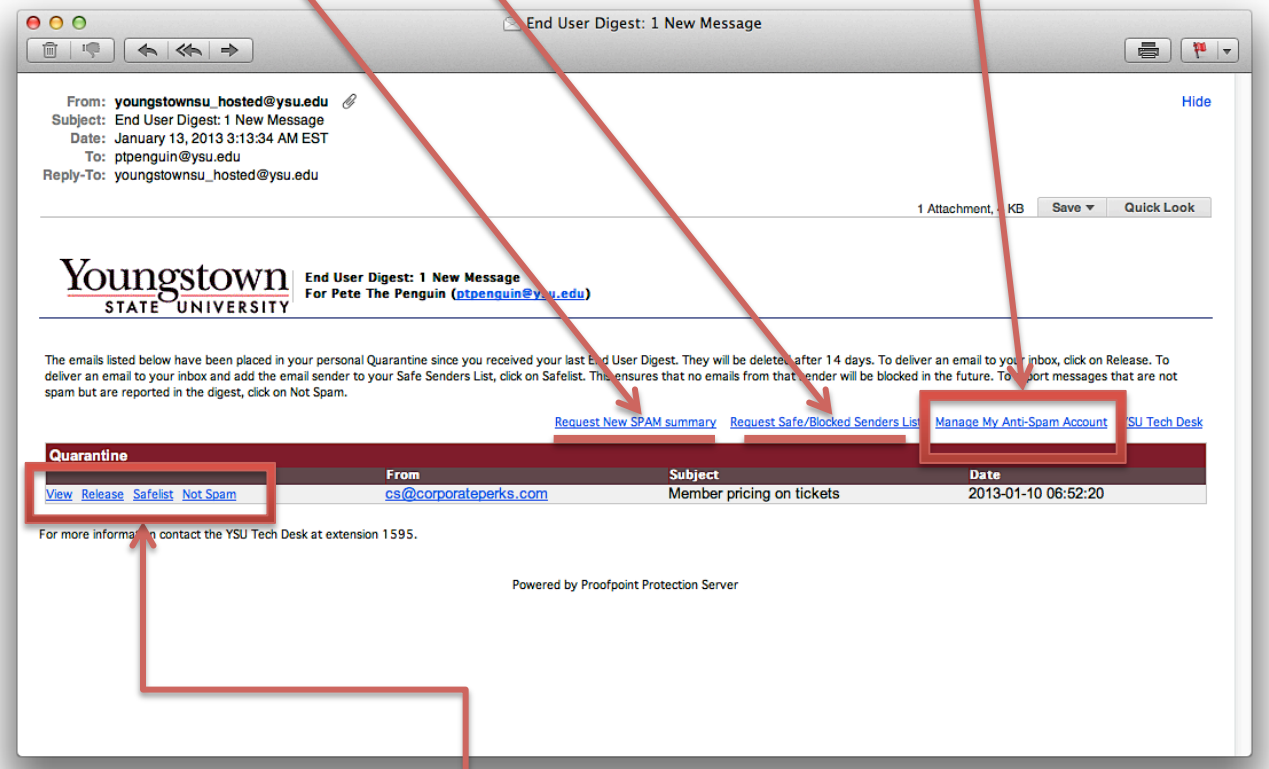
The Tech Desk recommends that users disable additional spam filtering tools such as SpamAssassin or any detection technologies built in to applications such as Microsoft Outlook. While additional spam filtering technologies are compatible with Proofpoint, using two or more spam detection tools may interfere with the delivery of the End User Digest or cause legitimate e-mail messages to be misplaced.

Using the Proofpoint End User Digest

By clicking on the various email links in the Proofpoint End User Digest email sent once a week, your Proofpoint anti-spam account can be configured and managed. A Proofpoint End User Digest email message is shown below with descriptions of its functions.

You can also request a new spam summary by clicking on the **Request New SPAM summary** link or see what email addresses are in your safe and blocked sender lists by clicking on **Request Safe/Blocked Senders list**

Click on the **Manage my Anti-Spam Account** link in your e-mail digest to be taken to the Proofpoint login window.



You can also click on one of the quick links to:

View: See the message in the Proofpoint web interface
Release: Release the message from the quarantine to your mailbox
Safelist: Add the message sender to a whitelist so that their messages are not blocked again
Not Spam: Mark the message as not spam

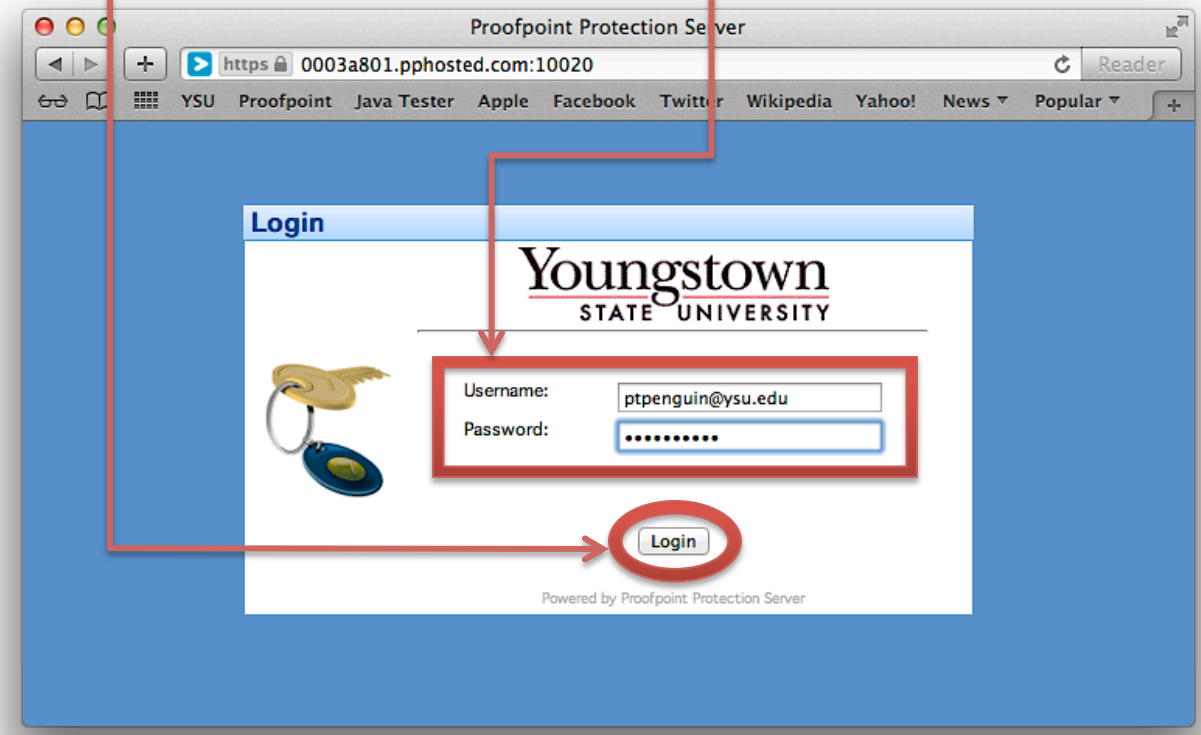
Logging into the Proofpoint Protection Server

Proofpoint can be accessed via a link in a Proofpoint End User Digest email, a link on the YSU website, or by manually entering the URL https://0003a801.pphosted.com:10020/ into the address bar of a web browser. The login page is shown below.

Enter the following information to log into Proofpoint:

Username: Your full email address ending in @ysu.edu
Password: Your YSU directory account password

Click **Login** to continue.



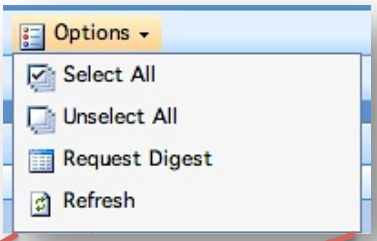
Using the Proofpoint interface - Quarantine

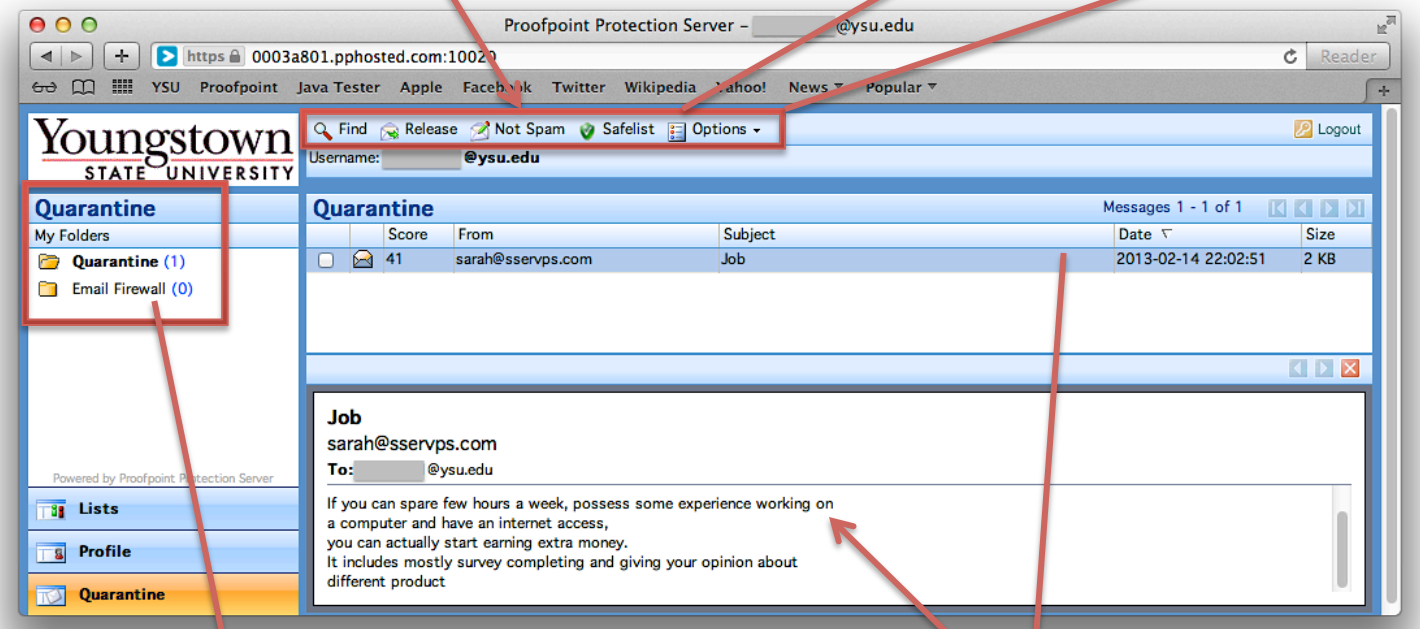
Once logged into Proofpoint, there are three sections on the bottom left that can be navigated to: **Lists**, **Profile**, and **Quarantine**. The **Quarantine** section is the default view upon log in and is where any held messages reside.

Find: Search for message(s)
Release: Release the message from the quarantine to your mailbox
Not Spam: Mark the message as not spam
Safelist: Add the message sender to a whitelist so that any messages from them to you are not blocked in the future

In addition to manually checking the box next to messages in the list to perform these four options, the **Options** drop-down allows you to:

Select All: Select all messages in the current view
Unselect All: Deselect all messages in the current view
Request Digest: Request that a current End-User Digest be sent to you
Refresh: Refresh the current page





Mail may be quarantined by the standard **Quarantine** or be in the **Email Firewall** – be sure to check both areas for held email.

When a message is selected from the list (it will now have a blue highlight in that row), a preview of it opens up in the lower portion of the message list area.

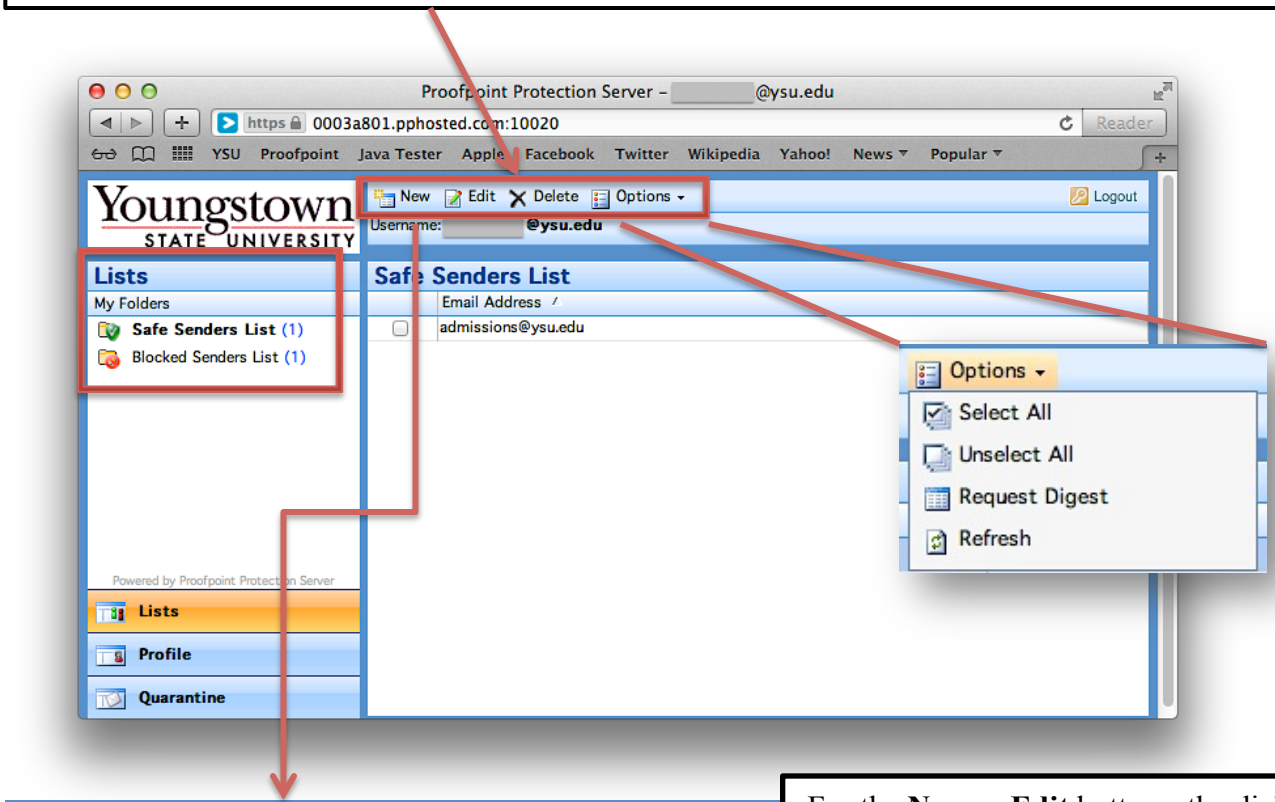
Using the Proofpoint interface - Lists

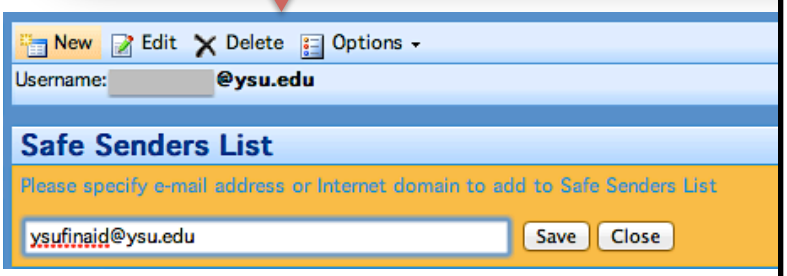
The **Lists** section contains your **Safe Senders List** and **Blocked Senders List**. These lists hold the addresses and/or Internet domains that are specified to be always allowed or always blocked by Proofpoint.

New: Add an email address or Internet domain to the selected list
Edit: Modify the currently selected email address or Internet domain in the selected list
Delete: Remove the currently selected email address(es) or Internet domain(s) from the selected list

In addition to manually checking the box next to messages in the list to perform these four options, the **Options** drop-down allows you to:

Select All: Select all messages in the current view
Unselect All: Deselect all messages in the current view
Request Digest: Request that a current End-User Digest be sent to you
Refresh: Refresh the current page





For the **New** or **Edit** buttons, the dialog will ask for either an email address in the format of **username@domain.com** or a web domain in the format of **subdomain.domain.com**

Click **Save** to save changes or **Close** to discard changes.

Using the Proofpoint interface - Profile

The **Profile** section contains your account settings and preferences. Default settings for the **Settings** subsection are shown below. The **Account** subsection simply displays the name and email address associated with the currently logged in Proofpoint account.

Send digest with new messages in my End User Digest: Ensure this is checked to receive a weekly End User Digest email when email messages are in Proofpoint (Default is '**Yes**')
Send digest with new messages in my End User Digest: Check this box to receive a weekly End User Digest email even when no email messages are in Proofpoint (Default is '**No**')

Preferred Language: The preferred language for the Proofpoint interface can be set here (Default is **'English (US)**')

What type of spam detection do you want? Please select a policy from the list below:
Default – This is the default and recommended spam policy.
No filtering Users Opted Out – This policy can be chosen if you would like your YSU mail account to be excluded from Proofpoint filtering.
Note: If you are having issues with a filter or policy, the Tech Desk (330-941-1595) would be your first point-of-contact to see if they can be addressed before you completely opt out of filtering
Global Spam Policy – This policy is the same as the **Default** spam detection policy.