Preface

About this Guide
This guide provides introduces end-users to Proofpoint Essentials.

Intended Audience and Prerequisite Knowledge
This guide is intended for end-users who interact with Proofpoint Essentials through a quarantine digest or by accessing the web-based user interface to manage personal preferences.

Important Terms
There are several terms used in this document that are highlighted here for reference.

Organization
• The term “organization” refers to your type of account your company has been setup within Proofpoint Essentials.

Organization Administrator
• A type of user who is responsible for managing the “organization”.

End-User
• A type of user whose email is filtered by Proofpoint Essentials, receives a quarantine digest email and has rights to access Proofpoint Essentials to manage their personal preferences.

Quarantine
• A term used to describe email that is not delivered to its intended recipients and is instead held by Proofpoint Essentials due to either your companies spam settings or by a custom filter.

Quarantine Digest
• An email delivered on regular basis to users whose email is being filtered by Proofpoint Essentials when email intended for that user has been blocked for delivery.

Filter
• A feature that allows a company to analyze incoming and outgoing email and take action based on the contents of the email.

Safe Sender List
• A list of senders whose email should by-pass spam filtering and be delivered to the users inbox.

Blocked Sender List
• A list of senders whose email should be quarantined.
Using Proofpoint Essentials

Accessing the User Interface

The Proofpoint Essentials user interface is a secure web-based portal that you can use to:

- Manage your user information.
- Update your preferences.
- Create and manage your safe and blocked sender lists.
- Search your email logs.
- Access your Emergency Inbox.

Logging In

1. Open a web browser and navigate to the appropriate URL.
2. Enter your login email address and password.
   
   If you do not have a password, contact your company administrator.
   
   If you forgot your password, click the Get a New Password link and an email will be sent to you with further instructions.

Resetting your Password

1. Click on your name in the top right hand side of the screen.
2. Select Profile.
3. Type in your new Password in the Password field.
4. Type in your new Password in the Retype Password field.
5. Click Save.

Navigating the User Interface

Quarantine

The quarantine tab allows you to view your quarantined email. In addition, you can adjust the options to display additional email messages such as all email, email that has been cleared or blocked.

To view your Quarantine:

1. Click on the Quarantine tab.
   
   - A default email logs view will be returned.
   - This will show you any inbound quarantined email received yesterday or today.
2. To modify your results, select Type from the drop-down list.
   
   - Inbound: Will include emails that were sent to you.
   - Outbound: Will include emails that were sent by you.
3. Select Received from drop-down list.
   
   - Today and Yesterday
   - The Last Week
   - The Last 2 Weeks
   - The Last 30 Ways
4. Select Status from drop-down list:
5. **Click Search.**

Results are displayed on the screen.

You can include additional options when searching your logs, including:

- **From Address or Domain:** Type in an email address or domain (i.e. domain.com) to only display results that were sent from the address/domain specified.
- **To Address or Domain:** Type in an email address or domain (i.e. domain.com) to only display results that were sent from the address/domain specified.
- **Subject:** Type in the subject line of the email.
- **Categories:** Select Advanced Search to access this control. Check the categories you wish to include in your results.

To view a quarantined email:

1. Click on the View button next to email you wish to view.
   - **Download:** Will download a copy of the email to your local desktop.
   - **Release:** Will release the email so that it is delivered to your mailbox.
   - **Delete:** Will remove the email from your view of the quarantine.
2. Click on the Close button to close the email view.
   
   You can only view emails that have been quarantined.

To view more information about a quarantined email:

1. Click on the Details button next to email you wish to select.
   - **General Description:** Basic information about the email including the sender, subject and time stamp.
   - **Scan Information:** Scan results for both spam and virus analysis.
   - **Pre-Recipient Classification & Delivery Status:** Classification of the email and current status.
   - **Other Information:** Sending IP address, country and email size.
2. Click on the Close button to close the email view.

To take an action with a selected email:

1. Check the checkbox next to the email you wish to take action on.
2. Select the Actions drop-down list.
3. Choose the action.
   - **Release from Quarantine:** Will release the selected email from the quarantine.
   - **Resend (Instant Replay)*:** Will resend the selected message to the user inbox.
   - **Not Spam:** Will classify the email as not spam.
   - **This is Spam:** Will classify the email as spam.
• **Delete**: Will delete the email from the email logs.

4. Click Apply.

**Settings**

**Profile**

Use this page to update your personal information. You can also access this screen by clicking on your name in the header and selecting Profile.

To make changes to your profile:

1. Click on Settings tab.
2. Click on Profile tab.
3. Update your information.
4. Click Save.

**Aliases**

Use this page to view all the aliases addresses registered to your account. An alias is another email address that is registered to you. For example: jane.smith@seroom.com may also have the alias: jsmith@seroom.com. Emails to both addresses will arrive at Jane Smith’s inbox.

**Spam**

Use this page to make changes to your spam settings. Spam settings are used to determine how aggressive Proofpoint Essentials spam engines should be for your account. The default value is 7. Your company administrator may have changed this setting for all users and therefore it is recommended you contact your administrator if you wish to make changes.

To adjust your spam settings:

1. Click on the Account Setup tab.
2. Click on the Spam Settings tab.
3. Click on the slider control on your screen.
4. Drag the control to the left (more aggressive) or right (less aggressive).
5. Click Save.

There are additional options you can set on this page such as:

- **Quarantine Bulk Email**: this will treat bulk email (i.e., email newsletters, promotional offer from site you have given permission to market to you) as Spam and quarantine these emails.
- **Spam Stamp & Forward**: This will deliver all emails to your inbox regardless of whether they are classified as spam or not. The subject line of any email identified as spam will be modified to include **SPAM**.
- **Include Easy Spam Reporting disclaimer**: This will add a footer to all your inbound emails. The footer will include a link for you to report to Proofpoint Essentials that the email is Spam.
- **Cross check inbound DSN**: Performs additional email analysis on emails based on outbound delivery logs.

We recommend you do not change any of these settings without contacting your administrator beforehand.
**Digests**

This page allows you to change your quarantine digest delivery settings.

- **Enable digests for user**: Use this option to enable/disable digests.
- **Only include messages quarantined since the last Quarantine Digest was sent**: Use this option to only send out digests if new mail has been received.
- **Quarantine Digest delivery start time**: The first time of the day that the digest should be delivered.
- **Interval between digest checks**: Use this option to choose the frequency of digest delivery.
- **Retention period**: Use this option to choose how long mail will remain in the quarantine.
- **Timestamp of last Quarantine Digest Check**: The timestamp of the last digest delivered to you.
- **Include emails that have been quarantined by**: Will add emails quarantined as a result of a filter or sender list to the quarantine digest.

Your company administrator has defined the quarantine digest settings. Any changes made will apply to you only. The administrator can reset these settings back to their defaults as needed.

To adjust your digest settings:
1. Click on the Settings tab.
2. Click on the Digests tab.
3. Update your settings.
4. Click Save.

**Groups**

This page will display any groups that you belong to.

**Sender Lists**

Sender lists allows you to define senders (someone@domain.dev) or domains (domain.dev) that you wish to either receive or block email from.

To add an entry to the Safe/Blocked sender list:
1. Click on the Settings tab.
2. Click on the Sender Lists tab.
3. Type in an SMTP address (user@domain.dev) or domain (domain.dev) You can add more than 1 entry by separating them with a comma or semi-colon.
4. Click Save

To remove an entry from the Safe/Blocked sender list:
1. Click on the Settings tab.
2. Click on the Sender Lists tab.
3. Highlight the entry you wish to remove and hit delete using your keyboard
4. Click Save.

**Disclaimer**

A disclaimer is a block of content that will be added to all your outbound emails. This is only applicable to companies who send outbound email through Proofpoint Essentials. You should contact your company administrator if you wish to use disclaimers.

To add/edit a disclaimer:
1. Click on the Settings tab.
2. Click on the Disclaimer tab.
3. Type in the content you wish to include as your disclaimer.

*The HTML editor allows you to use colors, customize fonts, include images, etc. The Plain Text editor only supports text.*

**Emergency Inbox**

The Emergency Inbox allows users to send and receive email when their company mail systems are offline, either for planned maintenance or an unexpected outage. The Emergency Inbox will automatically begin populating your email when your mail systems stop receiving email. And will clear out once your systems are functioning again. You should contact your company administrator to learn more about when to use the Emergency Inbox.

**Additional Features**

**Email Archiving**

If your company is using the Email Archive feature than you have the ability to search your own archived email. This means you can search emails that you have sent or received.

To search your archive:
1. Click on the Archive tab.
2. Enter the appropriate criteria for your search.
   - *Date / From:* Select the FROM date of the range you are interested in.
   - *Date / To:* Select the TO date of the range you are interested in.
   - *Date Type:* Choose either send date, received date or archived date.
   - *Search By:* Choose the location of the message area you wish to search; includes: Subject, Body, To, From, CC, BCC, attachment body, and attachment name.
   - *Matches:* Choose the relationship between the terms defined; includes: Any of these words (OR), All of these words (AND), and None of these words (NOT).
3. Click Search.

**Viewing Search Results**

Once you perform a search the system will execute the criteria against your archived data and return search results to the screen. You can further refine search criteria if necessary. There is a 1,000 record limit for search results.

Search results are displayed in a table and detailed information about each message is displayed including:

- Size (Kb)
- Sent date
- Received date
- Archive date
- From
- To
- Subject
To view a message:
  1. Click on the View link next to the message in question.

To download a message:
  1. Click on the Download link next to the message in question.

*Downloaded emails are in EML format.*

When viewing a message you can perform multiple actions for the message in question.

To view the list actions:
  1. Click on the Actions drop down.
  2. Select desired Option.

**Redeliver**
Provides users with the ability to have an archived email submitted to the Proofpoint Essentials email relay service for redelivery to each of the messages original recipients. The email will show up in the inbox of the original recipients in a matter of moments.

**Forward to**
Provides users with the ability to have an archived email forwarded to a desired email address. The email will show up in the inbox as an attachment from the Proofpoint Essentials Archive system.

**Export**
Provides users with the ability to have an archived email exported in an email format, which can then be managed by a Microsoft Outlook client as desired.
Email Encryption

If your company is using the Email Encryption service than your outgoing emails (emails that you send) may be routed to the Proofpoint Essentials encryption service. Depending on your how your company has configured email encryption this action may be triggered automatically or it may require you to add an identifier to email you wish to be encrypted. Both scenarios are explored below.

Encryption Scenarios

**Automatic Detection**

Your company may choose to scan outgoing email and look for content, such as credit cards numbers, banking information, etc. If an outgoing email is found to contain such content, the email is routed to the Proofpoint Essentials encryption service. There the email is stored and email notifications are sent to the recipients to direct them back to the encryption service where they can read and respond to your email. You will also receive a notification informing you that your email has been selected for encryption. When this happens you do not need to take any action. Your email has been sent and recipients will have a chance to respond.**Responses are delivered to your inbox.** You can also reply to responses you receive to your inbox. Replies will also be encrypted.

**Manual Detection**

Your company may provide you with instructions on how to manually trigger an email to be encrypted. This works in the same way described previously. In this case you will insert a term, likely in the subject line. Proofpoint Essentials will detect that term and as a result, route it to the encryption service. For example, you could insert the term “[Encrypt]” into your subject line ahead of your normal subject. As a result the email would be detected and routed to the encryption service and recipients will be sent notifications. You will receive an email notification informing you that your email has been selected for encryption. All replies will be delivered back to your inbox. In addition, the trigger term (i.e., [Encrypt]) is removed from your recipients email but is re-inserted back into replies to ensure that if you reply to a response, it too will be encrypted.