



# Getting Started with Email Archiving

Proofpoint Essentials

June 2017

## Important Information

The following information applies to all Proofpoint Essentials US data centers.

|                                                   |                                                                                                                                           |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| User Interface Access                             | <ul style="list-style-type: none"><li>• <a href="https://us1.proofpointessentials.com">https://us1.proofpointessentials.com</a></li></ul> |
| Email Archive IP Addresses (IMAP Connection only) | <ul style="list-style-type: none"><li>• 34.192.199.2</li><li>• 52.55.243.18</li><li>• 52.54.85.198</li></ul>                              |

## About

This document contains specific information related to setting up and managing the Proofpoint Essentials Email Archive (circa mid 2017). For additional information about the Proofpoint Essentials legacy email archive please refer to the Proofpoint Essentials Administrator Guide.

## Enable Feature

In order to launch the archive, the organization you are managing must have the Email Archive feature enabled.

To enable the Email Archive:

1. Click on Company Settings.
2. Click on Features.
3. Click the checkbox next to Enable Email Archive.
4. Click Save.
5. Click on Company Settings (to refresh the page).
6. Click on Archive.

*This will launch a new Email Archive tab in your email browser and automatically direct you to that tab.*

*If you are an existing Email Archive user, you may see another option on the Features page "Enable Legacy Email Archive". This setting controls access to the legacy archive product. This document applies to the new Email Archive, available as of June 2017.*

*If the organization you are managing has a legacy email archive, you will see two options presented. Choose "Launch Email Archive" to access the new archive or choose "Launch Legacy Archive" to launch the access the legacy archive.*

## Setup

To setup the archive you will need to:

1. Specify the organization's retention policy.
2. Add at least one connection..
3. Update user permissions to allow archive access.
4. Configure journaling.

All steps are performed in the Email Archive user interface.


To launch the Email Archive:

1. In the main toolbar, click on Archive.

## Specify Retention Policy

An organization's retention policy defines how long the organization's email should be retained in the archive. Proofpoint Essentials allows organizations to retain for between 1 and 10 years., after which time they will be automatically disposed.

To set an organization's retention policy:

1. In the Email Archive sidebar, hover over  (settings) and click Retention & Legal Holds.
2. Click and slide on the control to choose the desired email retention period that should be applied to the organization.
3. Click Save.

Company Legal Hold is an additional retention setting that will suspend disposition of all messages. Note that subsequently disabling this setting will cause **any emails that are older than the defined retention period to be disposed.**

## Connections

A connection is required in order to identify how emails should be collected and archived. Proofpoint Essentials supports two connection options: IMAP and SMTP.



### IMAP (Internet Message Access Protocol)

- This connection method allows Proofpoint Essentials to connect to the location where the organization's journaling mailbox is located.
- This connection is over Port 993 (IMAP over SSL) or over Port 143.
- For this connection to be used, the organization must enable local journaling and target a local mailbox. In addition, the organization must support IMAP connections and allow Proofpoint Essentials IPs to access the environment where the Exchange mailbox is located.

### SMTP (Simple Mail Transfer Protocol)

- This connection method allows customers to remote journal their email to a unique SMTP address supplied by Proofpoint Essentials. This is the preferred method for connection: support is available for both Local Exchange and Office 365.

To add a connection:

1. In the Email Archive sidebar, hover over  and click on Connections.
2. Click the  (add) button.
3. Enter a description (e.g. Sunnyvale Office).
4. Choose a Connection Type
  - IMAP
  - SMTP (Office 365) – Select if the organization is using Office 365
  - SMTP (Local Exchange) – Select if the organization is using Exchange locally

#### If IMAP selected:

1. Enter the server name to which Proofpoint Essentials should connect (hostname, IP address).
2. Enter the username of the account that should be used to connect to the mailbox.
3. Enter the password of the account that should be used to connect to the mailbox.
4. Enter the Port (Port 993 recommended).
5. Click Save.


#### If SMTP (Office 365) selected

1. Enter the undeliverable journal address that you defined when configuring Office 365 (See Appendix A).
2. Click Next.  
*A response will be returned, providing you with a unique SMTP address. Please copy this address and make note of it as you will need it to complete the SMTP configuration.*
3. Click Done.

#### If SMTP (Local Exchange) selected


1. Enter the IP addresses of the locations from which SMTP requests will be coming. For example, if requests are coming from a specific office location, you should enter the external IP address(es) of the office so that Proofpoint can accept connections from this location. You can enter more than 1. CIDR ranges are also supported.
2. Click Next.  
*A response will be returned, providing you with a unique SMTP address. Please copy this address and make note of it as you will need it to complete the SMTP configuration.*
3. Click Done.

### Test a Connection (IMAP Only)

Before you enable the new IMAP connection, you can test it to ensure that Proofpoint Essentials can successfully connect to the organization using the settings you have defined. To test a connection, click  (test).

The status icon will change and indicate that it is attempting a test. If the test is successful, the status icon will change to green. If unsuccessful, it will change to red. Hover over the red status icon to see the error response

### Enable/Disable a Connection

New connections are disabled by default. They can be enabled once you have tested the connection (IMAP) and are ready to begin archiving. To enable or disable a connection, click on  (enable/disable).

## Users and Access

The Email Archive syncs users from the Proofpoint Essentials account. Therefore all users added to the organization are automatically reflected in the Email Archive. Changes to users are reflected in the Email Archive every 5 minutes.


Users in the Email Archive can be granted additional permissions. By default, all users are "End-Users", meaning they have rights to search their own archived emails only.

| Role           | Permission                                                                                                                                                                                 |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| End-User       | Can access the archive and search their own email.                                                                                                                                         |
| Discovery User | Can access the archive, search all mailboxes and export email from the archive (available Q3 2017).                                                                                        |
| Administrator  | Can configure the archive (Connections, Retention& Legal Hold, manage users).                                                                                                              |
| Inactive User  | Has no access to the archive: this role is automatically assigned to a user who has been removed from the organization, either through a hard removal or due to a AD/Azure AD sync update. |

To view a list of archive users:

1. In the Email Archive sidebar, click on  (users).

### Grant user additional permissions

1. Click the  (edit) icon next to the user you wish to edit
  - o Check the Administrator box to grant the user administrator rights
  - o Check the Discovery User box to grant the user discovery user rights
2. Click Save.

## Search

Proofpoint Essentials allows all users with search rights to search archived emails using the following criteria:

- o Senders (From address)
- o Recipients (To address)
- o Content (including email subject email body and attachments)
- o Attachment name and extension
- o Date

These criteria can be used separately or combined to create a more complex search request.

# Access Email Archive

Users access the Email Archive through the Proofpoint Essentials user interface.



## Sign in to the Proofpoint Essentials Interface

1. Open an Internet browser on your computer and enter the interface URL.
2. Login using your supplied credentials.
3. Enter your username (your email address).
4. Enter the password supplied in the welcome email.
5. Click Archive.

*If your organization has a legacy email archive, you will see two options presented. Choose "Email Archive" to access the new archive or choose "Legacy Archive" to access the legacy archive.*

## Compose a Search

To get started, simply type in the name or words you would like to search for.

1. In the Email Archive, click  (search).
2. Type a name into the search field. *(For example, if you are searching for emails sent to Jane Doe, type Jane Doe.)*
3. Select "To" from the drop-down.
4. Type in another word to add to your search. *(For example, if you are searching for emails that contain the phrase hope project, type "hope project".)*
5. Select "Content" from the drop-down.
6. Click  (calendar) to add date information to the search criteria. *(For example, if you want to search for emails sent/received the current month, select "this month").*
7. Click on the date drop-down and select the date parameter.
8. Click Search.

When searching for multiple words or multiple content, users can choose one of the following operators.

| Operator | Description                                                                                                                                                                              |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ALL OF   | This will return emails that contain ALL OF the terms entered. For example, a search for ALL OF "this" or "that" will return emails if they contain both the terms "this" and "that."    |
| ANY OF   | This will return emails that contain ANY OF the terms entered. For example, a search for ANY OF "this" or "that" will return emails if they contain the term "this" or "that."           |
| NONE OF  | This will return emails that contain NONE OF the terms entered. For example, a search for NONE OF "this" and "that" will return emails if they don't contain the term "this" and "that." |

## User Search Examples

| Search Request                                                                          | Search Parameters                                                 | Results                                                                                              |
|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Show me all my archived email                                                           | No search parameters required; click Search                       | All email associated with user is returned                                                           |
| Show me all my archived email from today                                                | Date: Today                                                       | All email associated with the user with send date equal to current date                              |
| Show me emails I sent to Jane Doe in the last month with the words "Hope" and "Project" | Date: Last month<br>To: Jane Doe<br>Content: "Hope" and "Project" | All emails sent to Jane Doe over last month with both words hope and project anywhere in the content |



## Discovery Search Examples

| Search Request                                                                                  | Search Parameters                                      | Results                                                                      |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------------|
| Show me emails sent between Jane Doe and Bill Smith                                             | To: Jane Doe, Bill Smith<br>From: Jane Doe, Bill Smith | All emails where Jane Doe and Bill Smith are either the sender and recipient |
| Show me any emails received by employees that contain the word "Confidential" in the last month | Date: Last month<br>Content: Confidential              | All email in last month with word "confidential"                             |

## Access Extended Search

In addition to simple search, users can also change the view search parameters.


To access extended search:

1. In the Email Archive, click .
2. Click  (extended search).
3. Enter search details into any of the relevant search parameter fields.
4. Click Search.



## Saving a Search

Users can save any search they create, in order to reuse it when necessary.

To save a search:

1. Perform a search (a search must contain criteria before it can be saved).
2. Click on  (saved searches) above the message list.
3. Enter a name for the saved search.
4. Click Save Search.

To access a saved search:

1. In the Email Archive, click on .
2. Locate the search you want to re-run.
3. Click .

# Appendix A: Configuring Journaling for Office 365

## About Remote Journaling

Office 365 provides a remote journaling functionality to send a copy of all mail sent or received by members of a defined security group to a remote SMTP address. Proofpoint provides you with the SMTP address to use for this configuration.

While Proofpoint has a highly redundant mail infrastructure for receiving journal reports, we recommend configuring the Office 365 notification feature to inform you if journal reports cannot be delivered for some reason.

## Configuring an Outbound Connector

A dedicated outbound connector must be created so that all Journaling traffic to the Journaling mailbox will be delivered directly to the Email Archive instead of getting routed through the Proofpoint Essentials Email Gateway.

1. Open the Office 365 Administration Portal.
2. Click Admin (in the toolbar) and choose Exchange (in the list on the left).  
The Exchange admin center appears.
3. Click mail flow (in the list on the left).
4. Click the connectors tab.
5. Add an outbound connector (click the "+" sign).
6. Select Office 365 from the From menu and Partner Organization from the To menu.
7. Click Next.
8. Enter a descriptive Name (and optionally, Description) for the connector.
9. Choose whether to have the connector turned on when you save it (check Turn it on).  
You can also edit the connector and check the box at any time.
10. Click Next.
11. Select "Only when email messages are sent to these domains", then click + and enter the fully qualified domain name of the mail server (e.g. us.earchive.cloud).
12. Click OK to return to the connectors screen.
13. Select "Use the MX record associated with the partner's domain".
14. Click Next.
15. Leave the default settings for TLS: "Always use TLS" and "Issued by a trusted certificate authority (CA)".
16. Click Next.  
A new screen opens, showing your configuration choices. To make any necessary corrections, click Back, otherwise click Next.
17. When prompted to validate the connection, click Validate.
18. Enter the email address to which a test message can be sent.
19. Validation results are shown. To dismiss the results, click Close.

## Configuring Office 365 to Remote Journal Message Data to Proofpoint Essentials

*Note: This step assumes you are enabling journaling for all users.*

1. Open the Office 365 Administration Portal.
2. Click Admin (in the toolbar), and choose Exchange (in the list on the left).
3. The Exchange admin center appears.
4. Click compliance management (in the list on the left).
5. Click the journal rules tab.
6. In the customer admin address area, click Select address, click Browse, and select an admin email account. **This**



account will receive notification of non-deliverable journal reports.

7. Add a new journal rule (click the "+" sign).
8. The Journal Rule screen appears.
9. In the Send journal reports to field, enter the email address of the journaling mailbox (e.g. 5er123acd-5432-123a-a0a1-d9348328b71@us.earhive.cloud).
10. Enter a descriptive Name for the rule (e.g. Journaling to Proofpoint Archive).
11. From the "If the message is sent to or received from..." list, choose Apply to all messages.
12. From the "Journal the following messages..." list, choose All messages.
13. Click Save.
14. When prompted to confirm that you want the rule to apply to all messages, click Yes.

## Appendix B: Configuring Remote Journaling for On-Premise Exchange Servers

### Understanding Exchange 2010 Journaling

In Microsoft Exchange 2010, message journaling can be enabled either for individual mailbox databases (each of which contains multiple mailboxes) or for the entire organization.

The contents of an entire database are archived, so if you want to archive only a subset of mailboxes, move them to a separate database for which journaling can be enabled.

If you choose to enable journaling for the entire organization, you use a Journal Agent on the Hub Transport server, through which all messages pass, to specify the location of the organization's journaling mailbox. Mailboxes can be identified through a filter based on security group name.

### Configuring Exchange Journaling

*Note: Remote Journaling should be enabled directly to Proofpoint Essentials SMTP address, not by using the forwarding rule.*

#### **To configure journaling for the entire organization:**

1. In the Exchange Management Console, expand Organization Configuration, then click Hub Transport.
2. In the Toolbox Actions pane, click New Journal Rule.
3. Enter a name for the journal rule in the Rule name field.
4. Enter the email address to which journal reports should be sent.
5. Make sure the Global option (in the Scope area) is enabled.
6. Make sure the Enable Rule box is checked.
7. Click New, then Finish.

## Appendix C: Configuring Journaling (Local Exchange)

### Creating a User Account and Journaling Mailbox

#### Introduction

You need to create a new user account and a mailbox to be used as the journaling mailbox. If you have separate Exchange Servers, you may need a separate user account/mailbox per storage group and/or Exchange Server.

The journal account should not have any size restrictions applied to it. In addition, no Exchange Server rules should be applied to the account, especially rules that might move or delete messages from the account or move them to another folder such as "Junk Mail".

*Warning: If you attach the journal mailbox to your personal Outlook, any rules configured locally will also be applied to the journal mailbox.*

It is recommended that you create the Journal mailbox on its own separate mailbox database. Use a mailbox database that is isolated from normal operations, avoiding impact on regular users. Make sure the database has enough capacity for at least two weeks' worth of journaled messages).

#### **Creating a User Account and Journaling Mailbox: Exchange 2010**

1. On your primary Exchange Server, open the Exchange Management Console.
2. In the tree, expand Recipient Configuration.
3. Right-click on Mailbox and choose New Mailbox.
4. Select User Mailbox and click Next.
5. Select New User and click Next.
6. Choose the Organizational Unit in which you want to create the account.
7. Enter the full user name and a user login name, for example, Archive.
8. Enter and verify a password. Set the username must change password, user cannot change password and password never expires options in accordance with your company's policies.  
Record the login name and password: you will need them when you configure the Archive Appliance.  
Note: If you allow the password to expire, you must change it manually and reconfigure the appliance each time it changes.
9. Click Next. For Mailbox Settings, leave the Alias at its default, ensure the correct Server, Storage Group and Mailbox database are selected.
10. Click Next. Confirm the configuration summary settings are correct.
11. Click New. Exchange System Manager will attempt to create the user account and mailbox.
12. Once the wizard has completed successfully, click Finish.
13. In the tree, click Mailbox. A list of mailboxes will be displayed.
14. Right-click on the mailbox and choose Properties.
15. On the Mail Flow Settings tab, select Message Delivery Restrictions.
16. Click Properties.
17. For "Accept message from", select "Only senders in the following list" and click Add.
18. Select the mailbox created earlier.
19. For "Reject message from", ensure "No senders" is selected.
20. Click OK, twice.
21. Log in to the new account using OWA so Exchange will initialize the mailbox.

#### **Creating a User Account and Journaling Mailbox: Exchange 2013/2016**

1. On your primary Exchange Server, open the ECP web portal: <https://localhost/ecp>.

2. Login using the Exchange administrator account domain, username and password.
3. On the left panel, choose the recipients.
4. Click the mailboxes on the right panel.
5. Click the + and select User Mailbox.
6. In the popup window, click New user.
7. Enter the Alias, First Name and Last Name for this account.
8. Browse to select the Organizational Unit in which you want to create the account.  
Note: if you leave this blank, this account will be created under the default organizational unit.
9. Enter the User logon name.
10. Enter and verify a password. Set the "Require password change on next logon" option in accordance with your company's policies.
11. Record the logon name and password: you will need them when you configure the Archive Appliance.
12. Browse to the Mailbox database in which you want to create the account.  
Note: if you leave this blank, the account will be created in the default mailbox database.
13. Click Save. The popup window closes and a list of mailboxes is displayed in the mailboxes list.
14. Select the mailbox you just created and click the Edit icon. A popup window appears.
15. On the mailbox features tab (left panel), in the Message Delivery Restrictions section, click View details.
16. For "Accept message from", select Only senders in the following list, click + and select the mailbox created earlier
17. For "Reject message from", ensure No senders is selected
18. Click OK, then Save.
19. Log in to the new account using OWA to have Exchange initialize the mailbox.

## ***Configuring Journaling: Exchange 2013/2016***

### **Understanding Exchange Journaling**

Message journaling can be enabled either for individual mailbox databases (each of which contains multiple mailboxes) or for the entire organization. This guide provides instructions on enabling journaling for your entire organization. It is recommended that the journal mailbox(es) be created on a separate mailbox database that is isolated from normal operations, avoiding impact on regular users. Make sure the database has enough capacity for at least two weeks' worth of journaled messages.

If you choose to enable journaling for the entire organization, you define a Journal rule through the ECP web portal, which will allow you to specify the location of the organization's journaling mailbox and the scope of mailboxes to which the rule applies.

### ***To configure journaling for the entire enterprise:***

1. In the Exchange server box, login to the ECP web portal with administrator account, <https://localhost/ecp>
2. Click compliance management in the left panel.
3. Click journal rules in the right panel.
4. Click the "+" icon to create a new journal rule.
5. Enter the email address of the journal mailbox in the "Send journal reports to" field.
6. Enter a name for the journaling rule in the Name field.
7. Choose the appropriate option from the "If the message is sent to or received from" list.
8. Choose the appropriate option from the "Journal the following messages" list.
9. Click Save.

## Configuring Journaling: Exchange 2010

### ***Understanding Exchange Journaling***

Message journaling can be enabled either for individual mailbox databases (each of which contains multiple mailboxes) or for the entire organization. This guide provides instructions on enabling journaling for your entire organization. It is recommended that the journal mailbox(es) be created on a separate mailbox database that is isolated from normal operations, avoiding impact on regular users. Make sure the database has enough capacity for at least two weeks' worth of journaled messages.

If you choose to enable journaling for the entire organization, you use a Journal Agent on the Hub Transport server, through which all messages pass, to specify the location of the organization's journaling mailbox. Mailboxes can be identified through a filter based on security group name.

### ***To configure journaling for the entire organization:***

1. In the Exchange server box, login to the ECP web portal with administrator account, <https://localhost/ecp>
2. Click compliance management in the left panel.
3. Click journal rules in the right panel.
4. Click the "+" icon to create a new journal rule.
5. Enter the email address of the journal mailbox in the "Send journal reports to" field.
6. Enter a name for the journaling rule in the Name field.
7. Choose the appropriate option from the "If the message is sent to or received from" list.
8. Choose the appropriate option from the "Journal the following messages" list.
9. Click Save.