proofpoint.

365 TOTAL PROTECTION

Migration Guide for Proofpoint Essentials Partners

Contents

Overview

The purpose of this guide is to document how to migrate a customer account (i.e., Essentials 'organization') from Proofpoint Essentials onto Proofpoint 365 Total Protection. It focuses on the steps involved in onboarding the capabilities included in Total Protection Plan 1 and Plan 2.

You can use this guide to migrate and onboard customers onto Total Protection Plans 3 and 4. However, the steps to configure the additional products are not covered in this guide. You can book an onboarding session with a member of the Presales team to assist. Please contact your Account team if you would like to book a session with Presales.

Migration Tool

Scope

The migration tool provides you with visibility to all your customers with an active account on Proofpoint Essentials within the Proofpoint 365 Total Protection control panel. This includes customers that may be located across different Essentials 'stacks'.

> ***NOTE**: If you have customers on both US and EU data centres, these customers will not be accessible in the same migration tool. You will have different partner accounts where you can view and migrate customers with that region.*

> ***NOTE**: If you are using Proofpoint Essentials (i.e., NFRs), be advised you will not be able to use the migration tool for your own Partner account. The migration tool is only available to migrate "organizations".*

Mail Service Providers

While all mail service providers are supported, the migration experience is different for Microsoft 365 customers. Please use the table below to determine the migration tool experience.

Mail Service Provider	You will see the customer listed on the migration screen	The customer account will be created on Total Protection and licenses assigned	You can migrate configuration settings from Essentials to Total Protection
Microsoft 365	Yes	Yes	Yes

Google Workspace	Yes	Yes	No, you cannot migrate settings from Essentials. You will need to manually copy over configuration settings.
Local / Hosted Exchange	Yes	Yes	No, you cannot migrate settings from Essentials. You will need to manually copy over configuration settings.
Other (i.e., Zimbra)	Yes	Yes	No, you cannot migrate settings from Essentials. You will need to manually copy over configuration settings.

What is migrated from the Proofpoint Essentials customer account?

The following settings are included in the migration process.

Setting	Additional Details
Primary domain	Additional domains associated to the Essentials account are not migrated. Domains associated with a Microsoft 365 tenant will be imported when connecting to the Microsoft 365 tenant. For non-Microsoft 365 customers, additional domains will need to be manually added.
Admin contact	First name, last name, email address, phone number
Customer-level sender lists (i.e., allow list, block list)	
User-level sender (i.e., allow list, block list)	
URL defense / domains and IP exclusion entries	
Anti-Spoofing Policies / DMARC exceptions	
Anti-Spoofing Policies / SPF exceptions	

Anti-Spoofing Policies / DKIM exceptions	
Branding – Color Scheme / Logo	If configured at the organization level

What is not migrated?

The following settings are not included in the migration process.

Setting	Additional Details
Quarantine	30-day quarantine remains in Proofpoint Essentials. Access to the customer's account in Essentials will remain for at least 30 days post migration in order to access the quarantine.
Email filter policies	Email filter polices will need to be manually created. Instructions are included below.
Groups	Groups are not migrated. They will need to be added manually to Total Protection.
Spam settings	Spam settings are not migrated.
Quarantine Digest settings	Quarantine digest settings are not migrated.
Attachment defense settings	
DKIM key	

***NOTE**: Only customers on the Business package or higher will be able to migrate their settings from Proofpoint Essentials. Customers on Beginner and Beginner + packages will need all to manually recreate their settings.*

Security Awareness

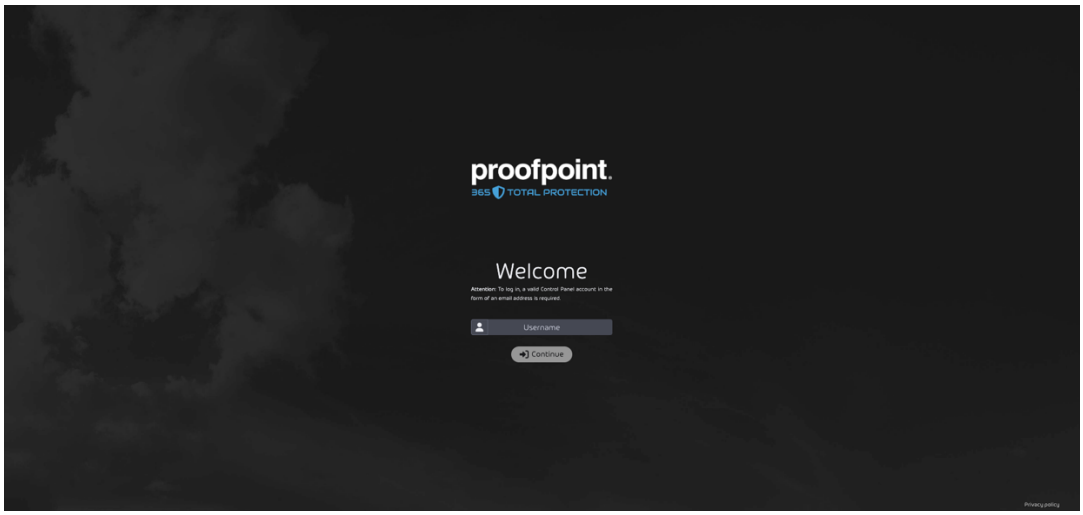
Customer accounts with an active Security Awareness subscription in Proofpoint Essentials will be assigned a Security Awareness subscription license in Proofpoint Total Protection. However, no configuration from the customers Proofpoint Essentials Security Awareness site is migrated to Total Protection.

Email Archive

You customer's email archive will not be migrated during this process. It will be performed at a later stage. To prepare for this, we recommend configuring the archive in the Control Panel before the migration. Instructions for setting up the archive are provided later in this guide. Access to the email archive through the Proofpoint Essentials console will remain available for the customer until it is migrated to Total Protection.

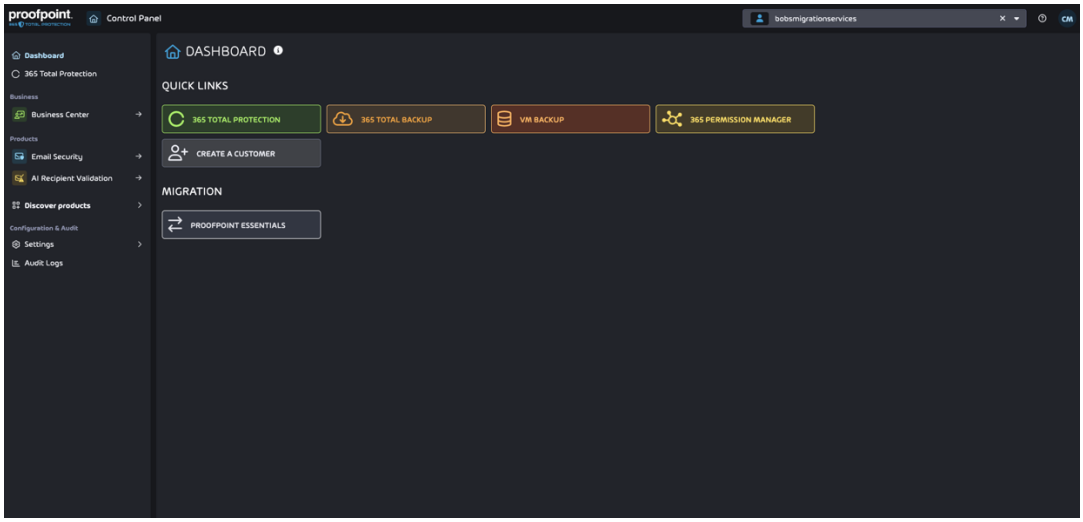
Getting Started

Start by logging into the Proofpoint 365 Total Protection control panel located at http://cp.proofpoint.com with your supplied partner credentials.

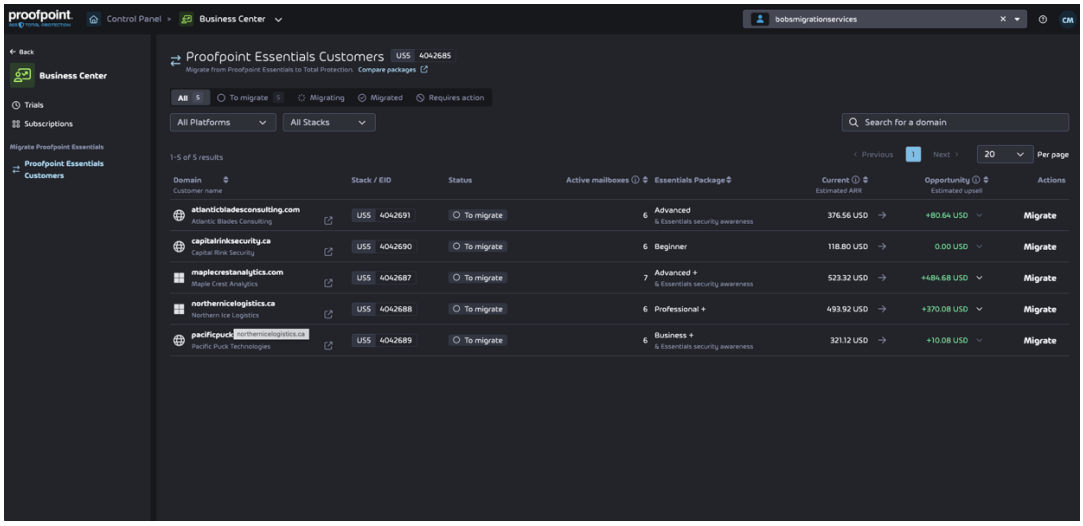


Once on the Main screen, click on “Scope Selection” in the top-right toolbar and select your partner account , then click on the “Business Center”, which will appear in the left-hand menu.

> ***NOTE**: If you cannot see Business Center listed, email migrations@msp.proofpoint.com to get it enabled for you.*



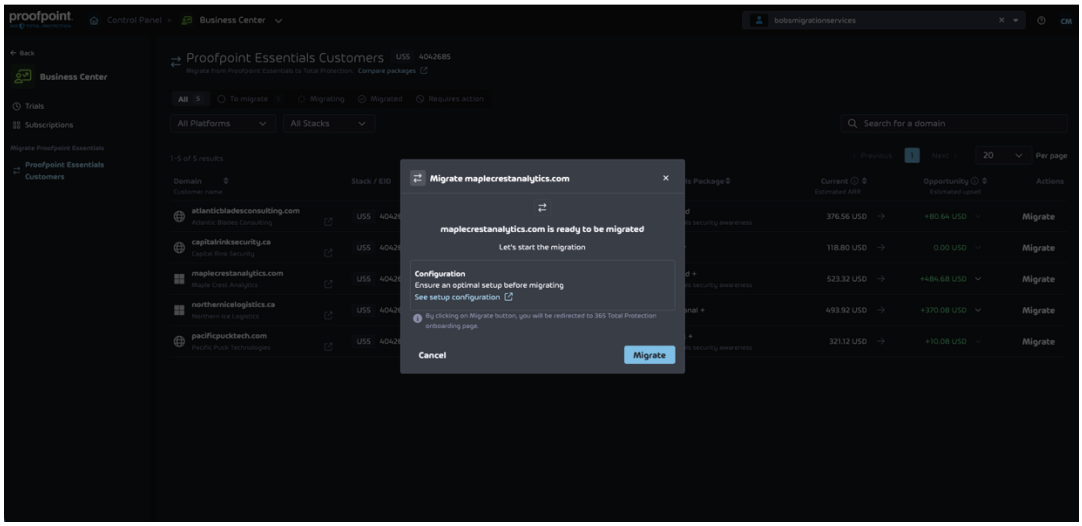
Now, click on “Proofpoint Essentials Customers”. This will direct you to the migration page where you we will see a list of all your customers along with details on their Essentials stack and unique identifier (EID), migration status, active mailbox counts, and current Essentials package.



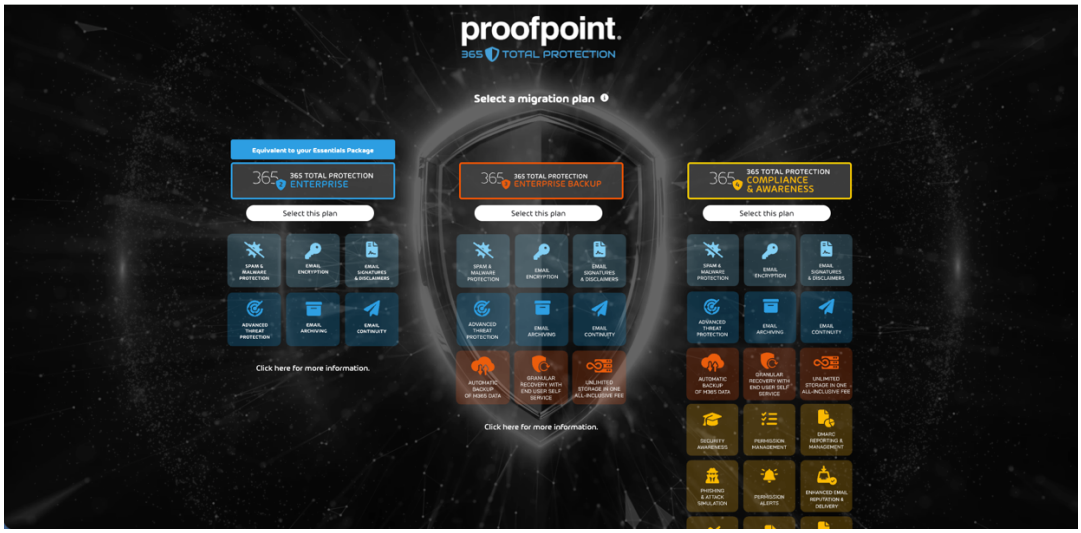
***NOTE**: This view includes all customers that are associated to your partner account on Proofpoint Essentials. This includes customers across different stacks. Different icons are used to identify Microsoft 365 and non-Microsoft 365 accounts.*

To migrate a customer, click the Migrate button next to the customer you wish to migrate.

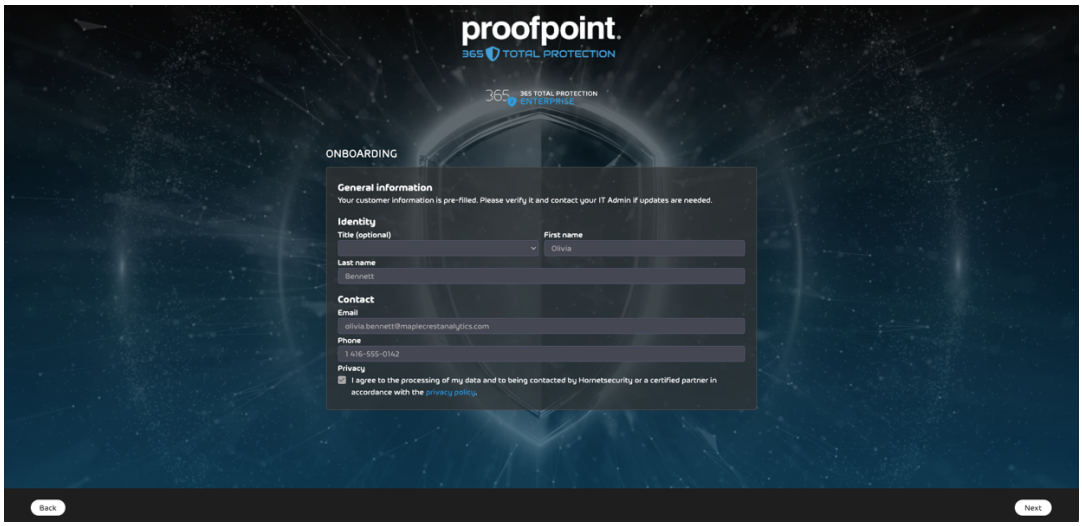
A pop-up will appear to confirm the migration. Click on See setup configuration link to open a new browser tab that contain useful details to move mail routing to the new platform. Click the Migrate button to proceed.



Next, click on the Total Protection plan you wish to select for this customer.

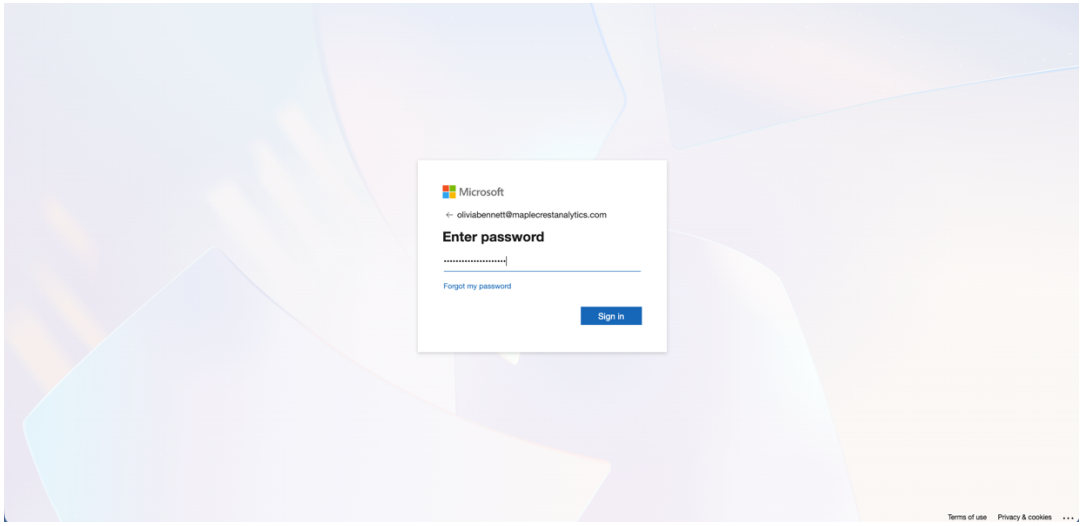


Next, you will see the Admin Contact associated to the customer in Proofpoint Essentials. Make sure the privacy checkbox is checked and then click the Next button.

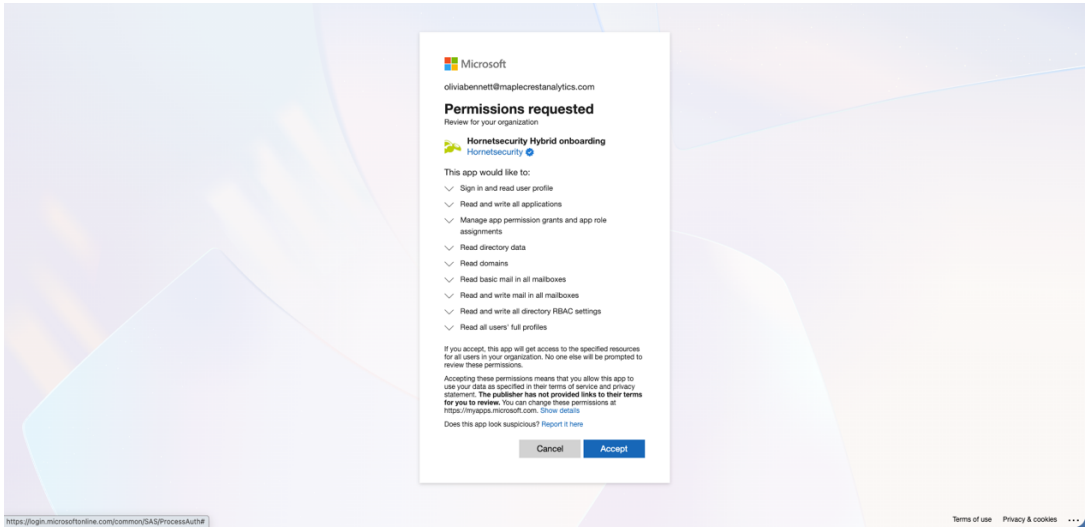


Next, choose Hybrid and then click the Configure Hybrid button.

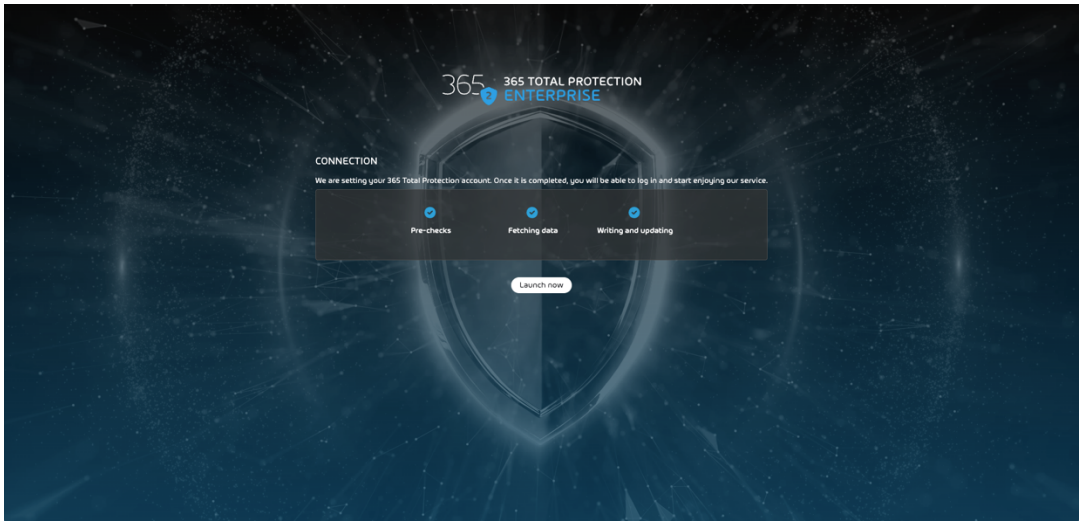
Next, you will be prompted to enter credentials for a Global Admin account associated to the customer account you are migrating.



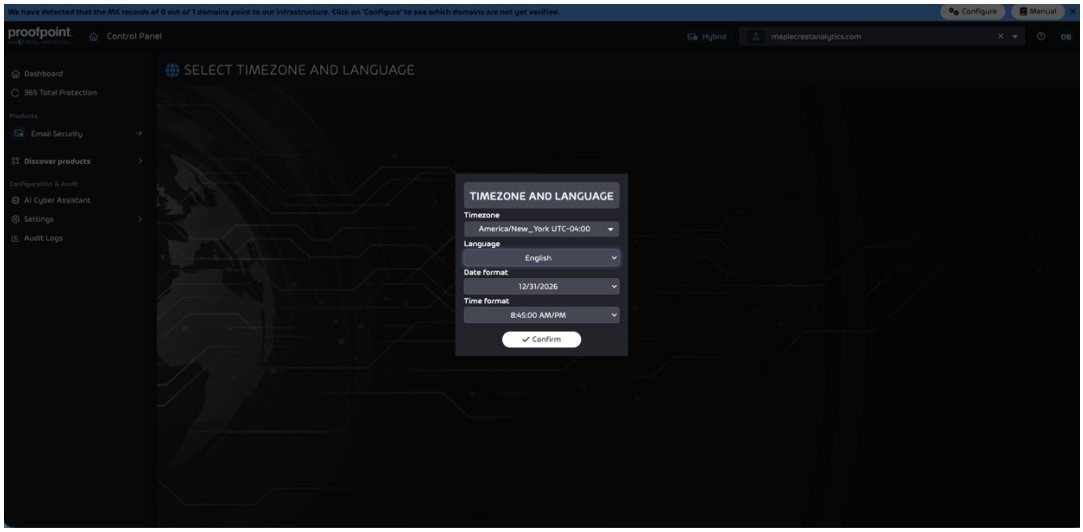
Next, click the Accept button to accept the permissions required.



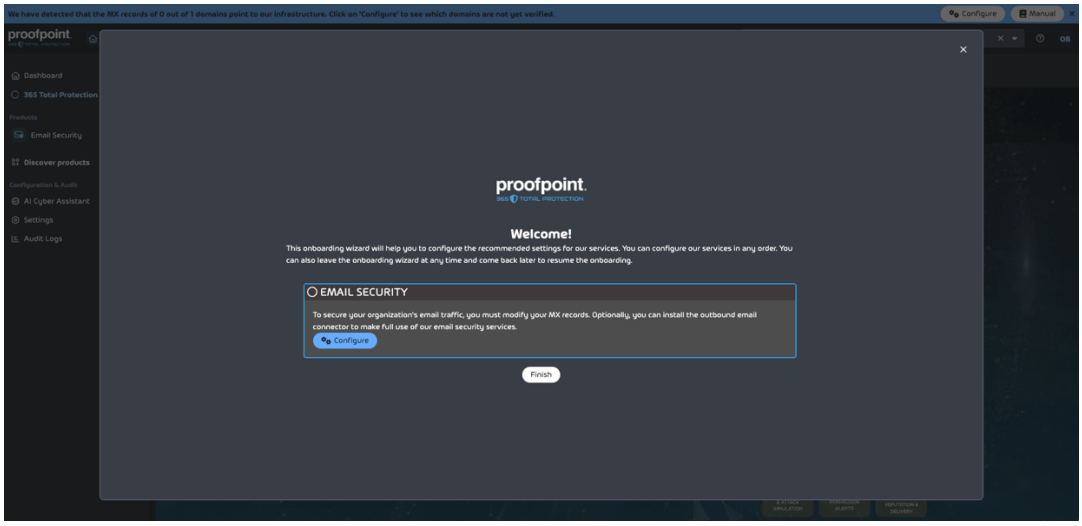
Once connected to the Microsoft 365 tenant, the tool will create the customer account. Once the steps are complete, click the Launch now button.



You will then be asked to update the regional settings for the customer account. Please make any adjustments and click the Confirm button.

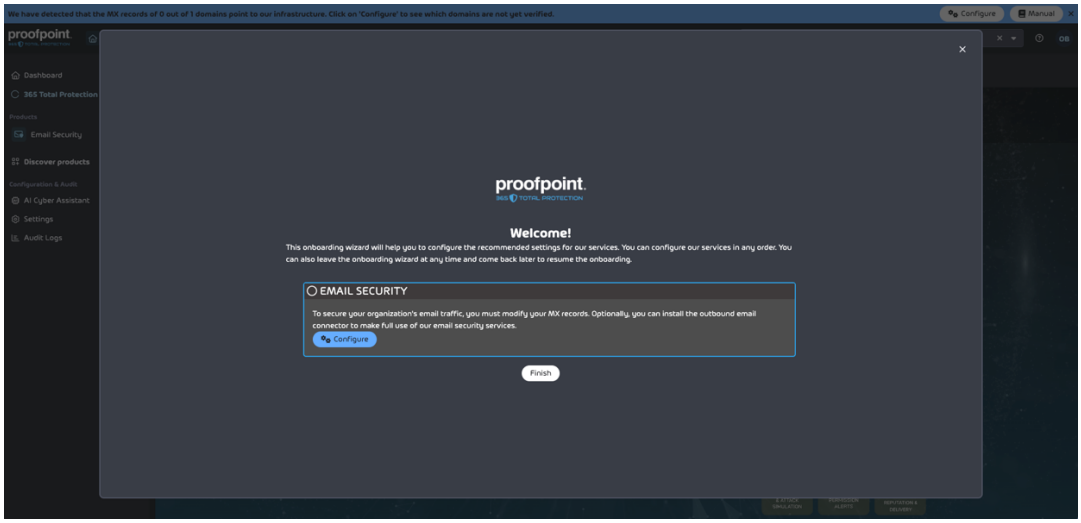


Now, you will be presented with the Onboarding Wizard. This wizard will guide you through the steps to import your customer's configuration from their Proofpoint Essentials account and complete remaining steps to onboard them onto Proofpoint 365 Total Protection.

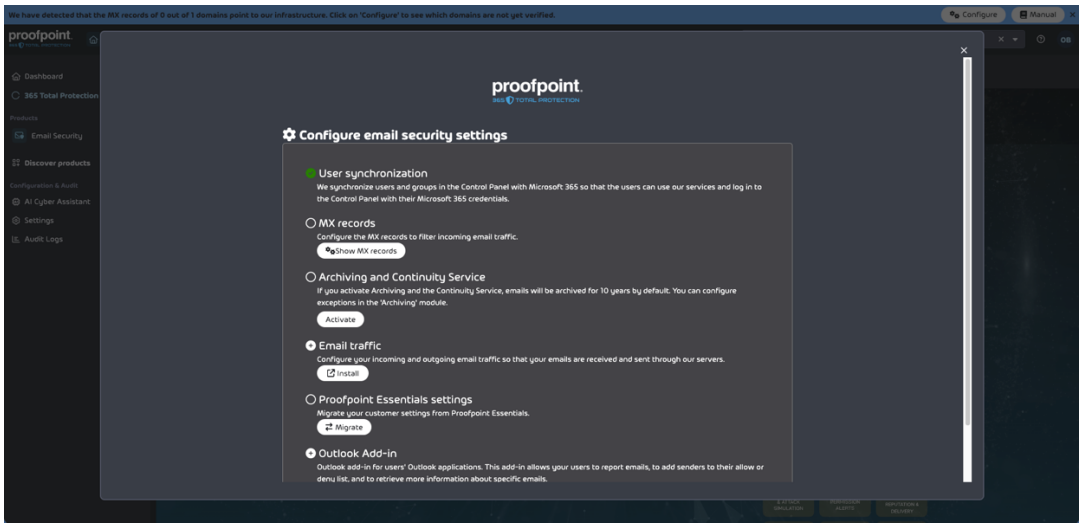


> ***NOTE**: You can close the wizard at anytime by clicking on the X button. You can resume the This will not cancel the migration.*

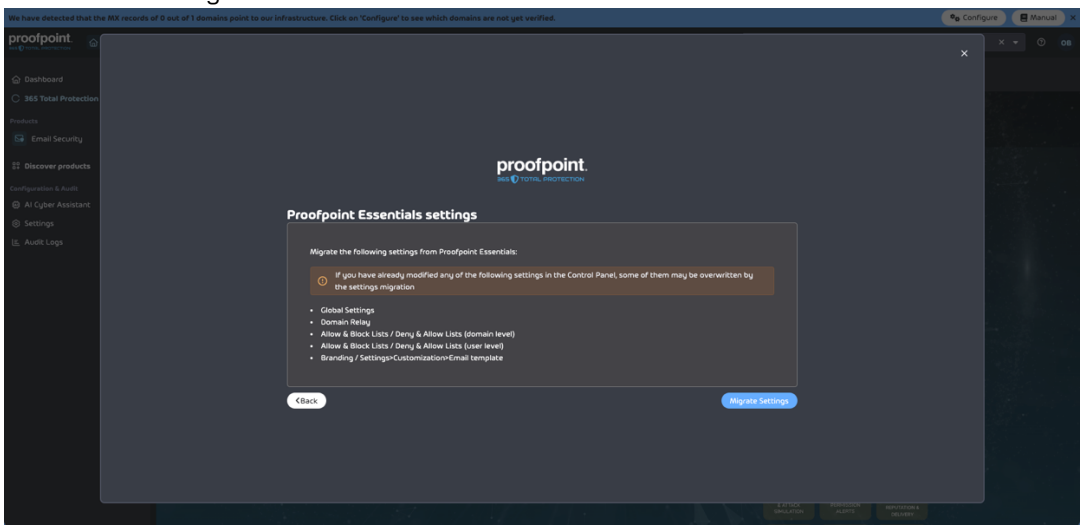
To proceed with the migration, click the Configure button in the Email Security service item presented.



Now, click on the Migrate button underneath the Proofpoint Essentials settings section.

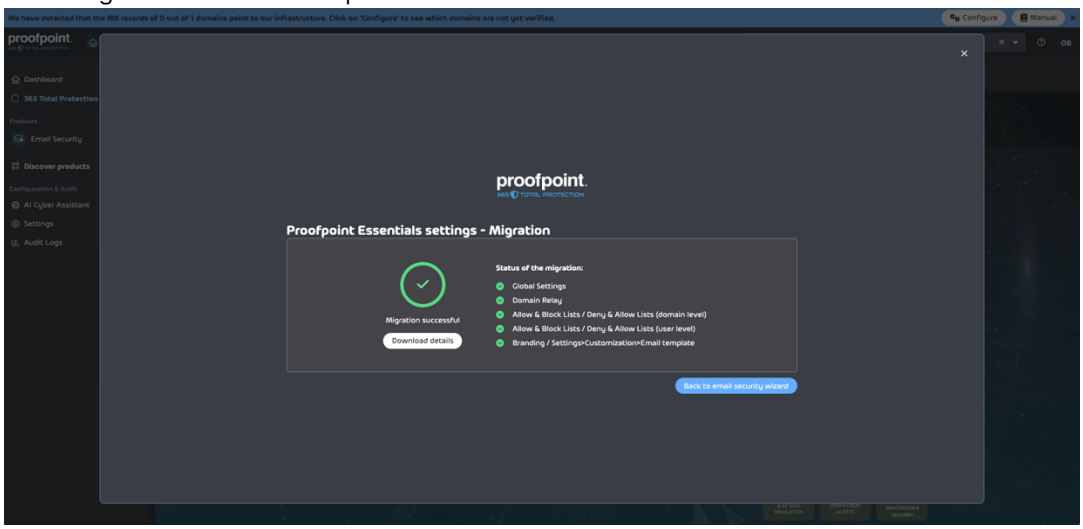


You will then see a Proofpoint Essentials settings migration screen. Click the Migrate Settings button to initiate the migration.



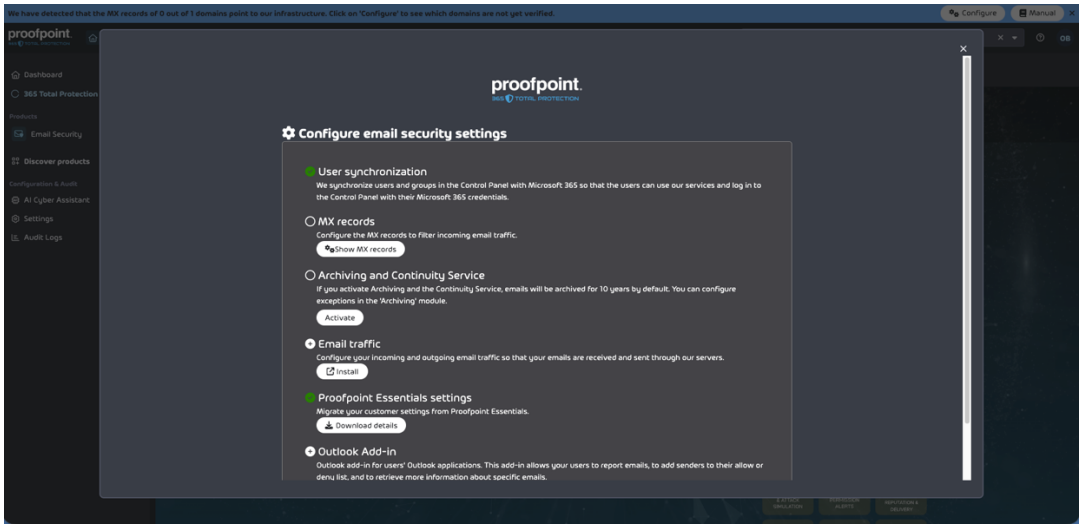
Once you initiate the migration, you will see a progress indication as it migrates selected configuration items from the Proofpoint Essentials customer.

Once is has completed, click the Download details button to download a summary of the migration that may be useful at some point.



> ***NOTE**: It is not unusual for certain allow and block list entries to fail to migrate based on some formatting differences between Proofpoint Essentials and Proofpoint 365 Total Protection. Use the migration results file to identify the failed records and you can manually add those entries.*

Once you have downloaded the file, click the Back to email security wizard button. You will see that the Proofpoint Essentials settings section has been marked as completed.

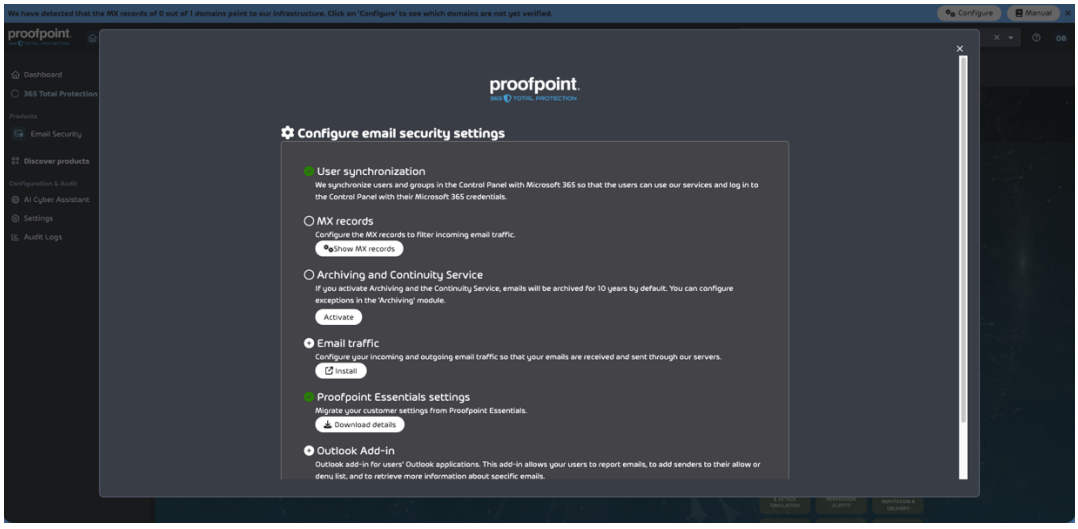


As mentioned previously, the migration tool will migrate the following:

- Admin contact & general customer information
- Allow & Deny List (For customer and end users)
- Anti-spoofing exemptions (DMARC, DKIM, SPF)
- Branding settings (If any, Logo, color, customer “From” email.)

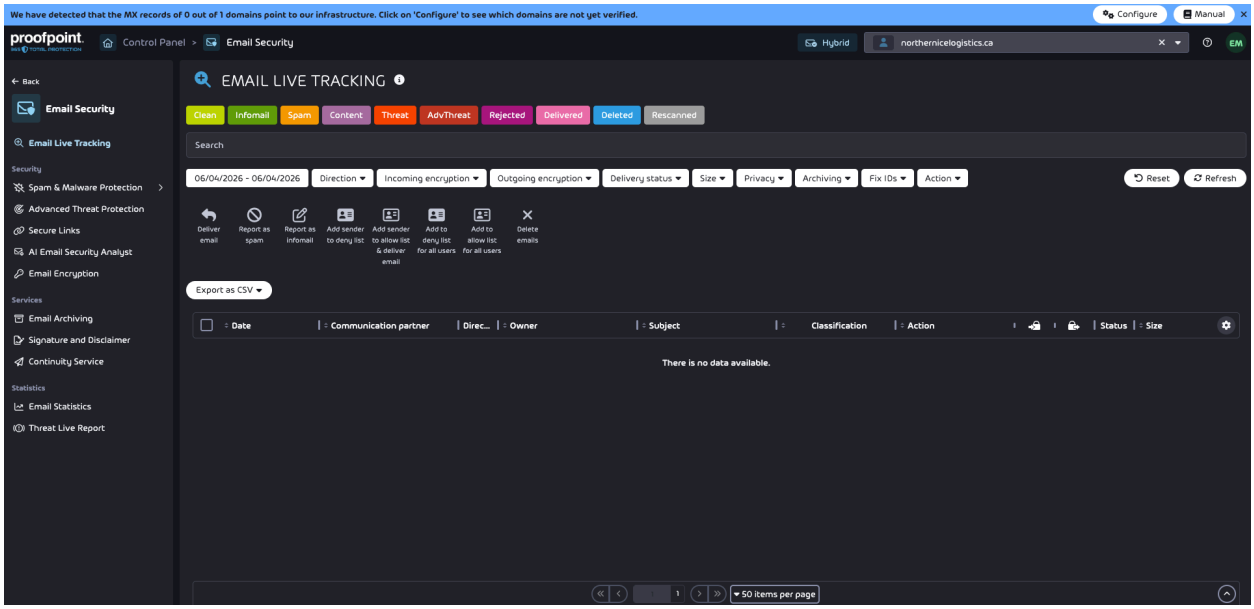
You will need to manually migrate additional settings that are not migrated (i.e., Email Filter polices). You can close the onboarding wizard, to manually migrate and configure these settings, before resuming the onboarding steps.

To close the wizard, click the X icon in the top right corner of the wizard.



This will take you to the 365 Total Protection plan page.

Click on Email Security in the left-side navigation to access the relevant email security configuration components.



Additional Configuration

The Proofpoint 365 Total Protection Control Panel includes extensive built-in documentation that provides an overview of each feature and configuration information. To access the documentation, click the question mark icon in the toolbar, followed by Manual.

***NOTE**: For each configuration name label that has been included in the steps, we have included the corresponding name from the Proofpoint Essentials console. For example: "Content Control (Filter Policies)" means that Filter Policies, as it is referred to in Essentials is referred to as Content Control in Proofpoint 365 Total Protection.*

Settings

Content Control (Filter Policies)

Content Control allows administrators to manage the handling of attachments of incoming and outgoing emails. Administrators can define a maximum allowed email size. Emails that exceed this size are filtered out. Furthermore, administrators can choose which attachment types shall be filtered out. The following attachment types can be selected:

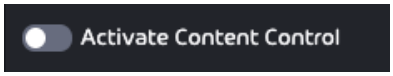
- Encrypted attachments
- Executable attachments
- Office files with macros

Additionally, administrators can forbid file types based on their file extension. Forbidden file types can be defined both for directly attached files and for files in archives. Moreover, categories can be used to forbid several file types at once.

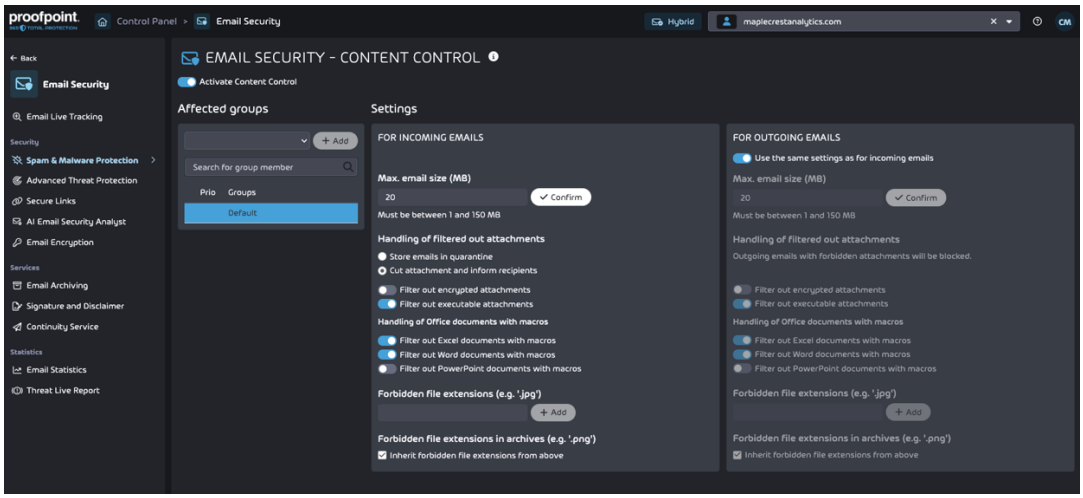
Administrators can choose whether the filtered-out attachments are stored in quarantine or whether the emails are delivered to the recipients without attachments. In the second case, the recipients are notified that the attachments have been cut off.

Settings can be made either for all mailboxes of the domain or for groups of mailboxes.

To active Content Control, click the Activate Content Control toggle.



Once activated, you can adjust your preferences for both incoming and outgoing emails.



Compliance Filter (Filter Policies)

Compliance Filter allows administrators to define their own filter rules, for example, to classify incoming emails as Clean, Spam or Threat. Furthermore, emails can be rejected, redirected through a different server or forwarded to other recipients.

The Compliance Filter can check both incoming and outgoing emails. After the activation of the Compliance Filter, administrators can define filter rules of the following types:

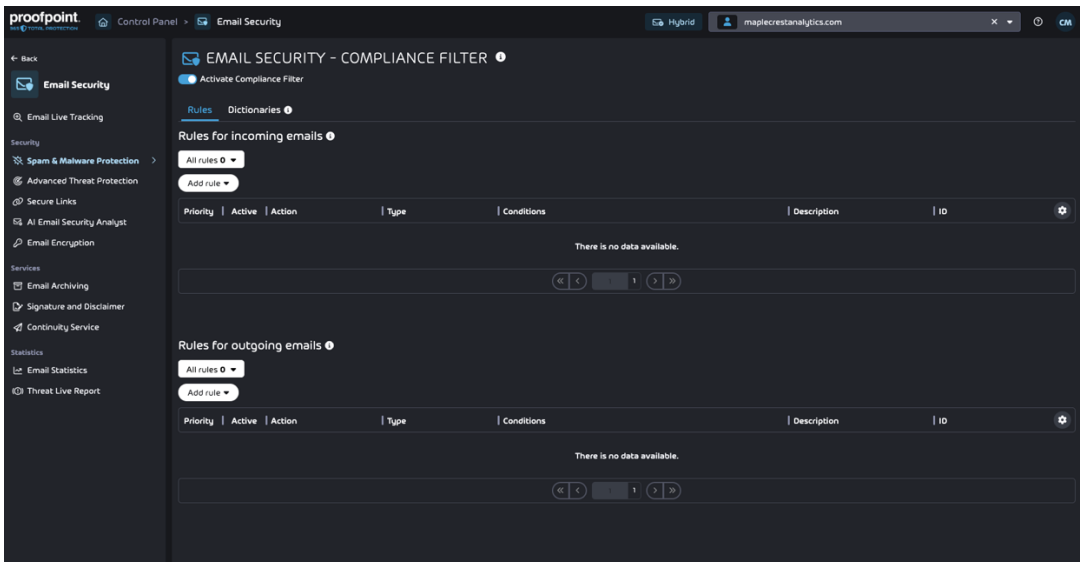
- Header
- Body
- Advanced

Regular expressions can be used in the conditions of the filter rules. Administrators assign an action to each filter rule. This action is automatically applied to the emails that match the filter rule.. In total, up to 1500 filter rules can be defined per customer.

Besides filter rules for individual expressions, more complex and precise filter rules can be created using dictionaries, each of which may contain up to 15000 literal expressions or up to 1000 regular expressions. Customer-level administrators can create and maintain up to 250 dictionaries for their primary domain. Dictionaries with regular expressions significantly reduce the effort required to create and maintain filter rules.

To active Compliance Filter, click the Activate Compliance Filter toggle.

Once activated, you can create filters for both incoming and outgoing emails.

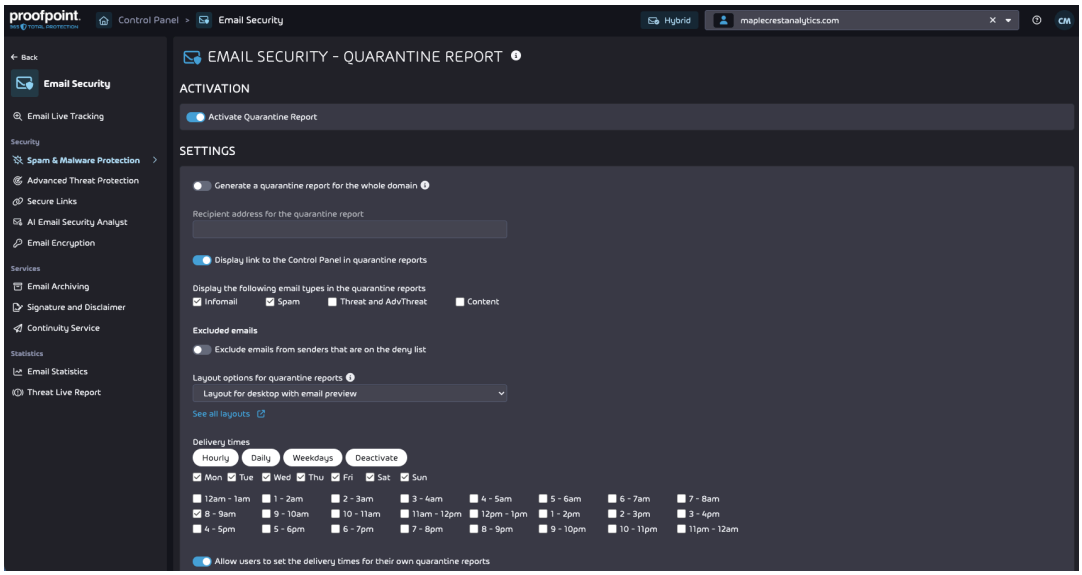


Quarantine Report (Digests)

A quarantine report is a report which is either created individually for a user or for an entire domain and is delivered to the recipient by email. The quarantine report lists all emails categorized as Spam and Infomail, as well as emails that have not been delivered to the user but put in quarantine. If the recipient of a quarantine report has the required permissions, they can later have those emails delivered on demand.

The Quarantine Report was activated by default.

You can adjust your preferences for the quarantine report.

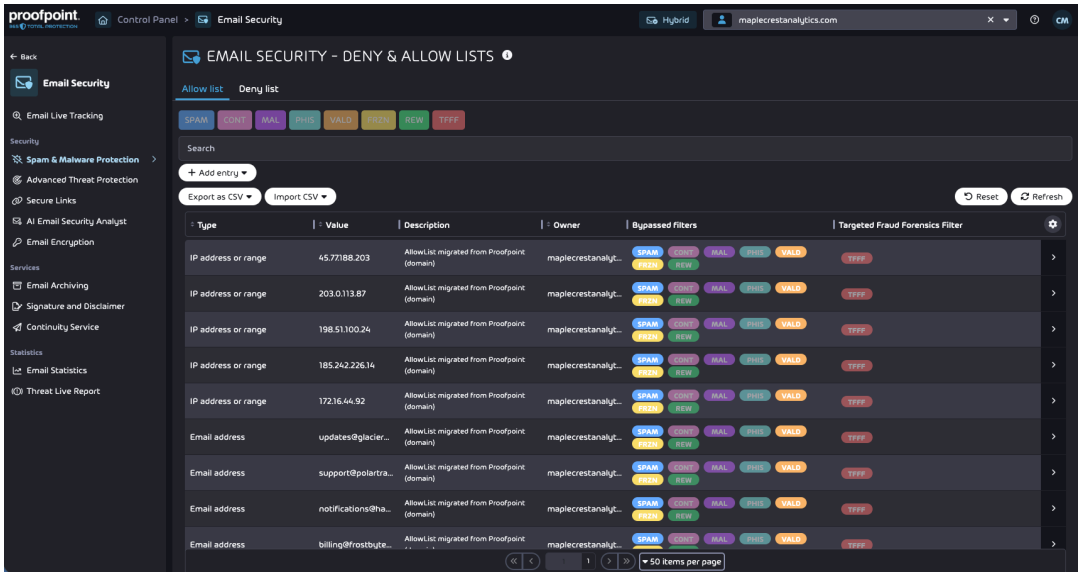


Deny & Allow Lists (Allow & Block List)

Deny & Allow Lists contains a user's or a customer's deny list and allow list. Each user has their own deny list and allow list, which they can manage themselves. Administrators can also access their users' personal deny lists and allow lists by selecting the users from the scope selection. Additionally, administrators can manage a deny list and allow list for their whole domain. The deny list and allow list at domain level shows not only entries that apply to all users of the domain but also entries of individual users of the domain.

With the deny list, users and administrators can define that certain incoming emails of a user or of all users of a customer are classified as spam by spam filtering. Emails classified as Spam are not directly delivered to the recipient. Instead, the action set up for Spam in the Spam & Malware Protection settings is executed by the product. This action can be: Hard delete, Quarantine or Tag.

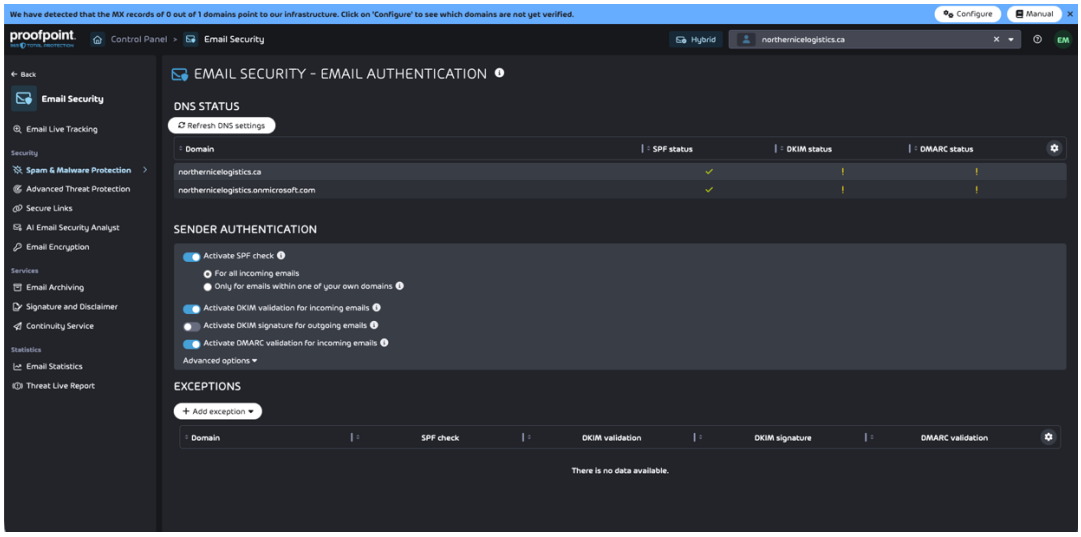
Your customers allow and deny lists were imported by the migration tool but you can add additional entries or edit existing entries as desired.



Email Authentication

Email Authentication offers different methods to authenticate email senders. The following methods are available:

- SPF check (Sender Policy Framework)
- DKIM validation and DKIM signing (DomainKeys Identified Mail)
- DMARC validation (Domain-based Message Authentication, Reporting and Conformance)



Outbound Settings

If you will be filtering your outbound email through Proofpoint 365 Total Protection, you will want to:

1. Update the SPF record for the customer's domain
2. Set new CNAME records in the DNS zone of the cutomer's domain

SPF Record
Option #1: Replace your existing SPF record to the Proofpoint 365 Total Protection SPF record. If you are performing this step during off hours, you can choose this option as there may be a minor disruption. If you are performing this change during business hours, option #2 is recommended.

- Type: TXT
- Name: @
- Value: v=spf1 include:spf.pp-tp.com ~all
- TTL: 1 hour

Option #2: Update your existing SPF record to include Proofpoint 365 Total Protection. This is the recommended approach to avoid any disruption in the cutover process.

- Edit your existing SPF record to add "include:spf.pp-tp.com" to the value. For example, if your SPF record has Proofpoint Essentials (v=spf1 include:_spf-us.ppe-hosted.com -all), you can modify it to the following: "v=spf1 include:_spf-us.ppe-hosted.com include:spf.pp-tp.com -all" which will designate both Proofpoint Essentials and Proofpoint 365 Total Protection as designated senders for the domain.

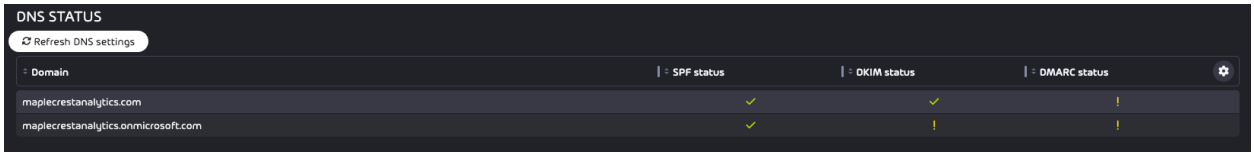
> ***NOTE**: Once mail services are completely cutover to Proofpoint 365 Total Protection, you can remove the legacy Proofpoint Essentials SPF record.*

DKIM Signing
You will need to add the following entries in the DNS zone of the customer's domain.

- CNAME Record 1:
  - Type: CNAME
  - Name: s1._domainkey.DOMAIN.TLD
  - Value: s1._domainkey.pp-tp.com
  - TTL: 1/2 hour

- CNAME Record 2:
  - Type: CNAME
  - Name: s2._domainkey.DOMAIN.TLD
  - Value: s2._domainkey.pp-tp.com
  - TTL: 1/2 hour

To verify both SPF and DKIM settings have been successfully added to the domain, view the DNS status section. If there are checkmarks next to the domain for both SPF status and DKIM status, you can proceed.



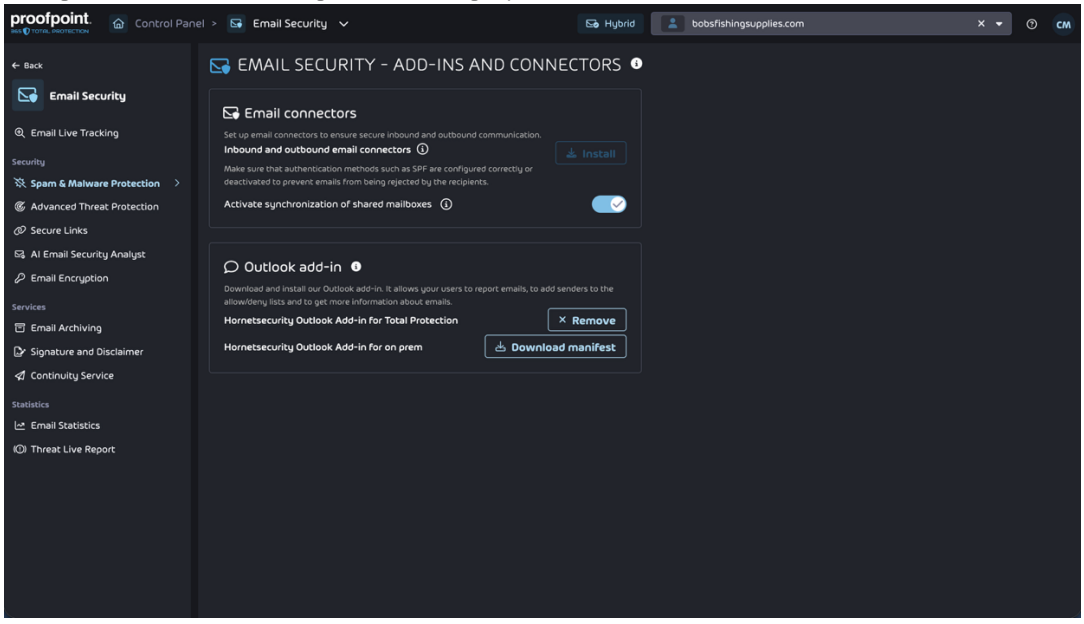
Once verified, you can enable the "Activate DKIM Signature for outgoing emails" toggle so that DKIM is applied to outgoing emails..

Functional Accounts / Shared Mailboxes

Functional Accounts are still monitored and protected after migration to Proofpoint 365 Total Protection. They do not need to be added into the customer control panel unless you want to deliver a quarantine report. If you want to deliver a quarantine report to functional accounts (shared mailbox, aliases, and distribution lists), you can enable automatic synching of your shared mailboxes.

> ***NOTE**: Automatic synching of shared mailboxes is available for Microsoft 365 only.*

Navigate to Email Security, followed by Spam & Malware Protection, then Add-Ins & Connectors.

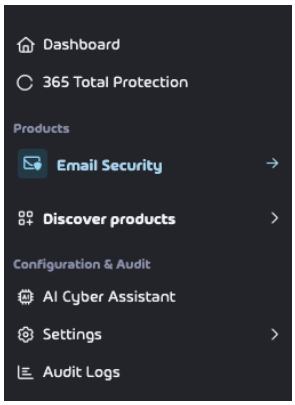


Click the control to activate the synchronization of shared mailboxes.

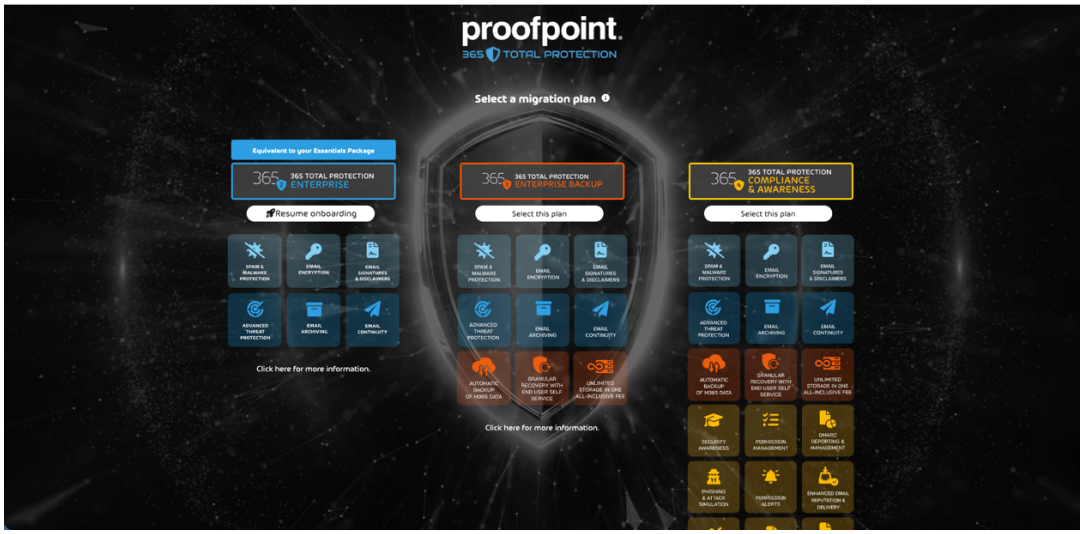
> ***NOTE**: This will require that you authenticate with the Microsoft 365 tenant with the same Global Admin account used earlier and will request you accept additional permission changes..*

Resume Onboarding

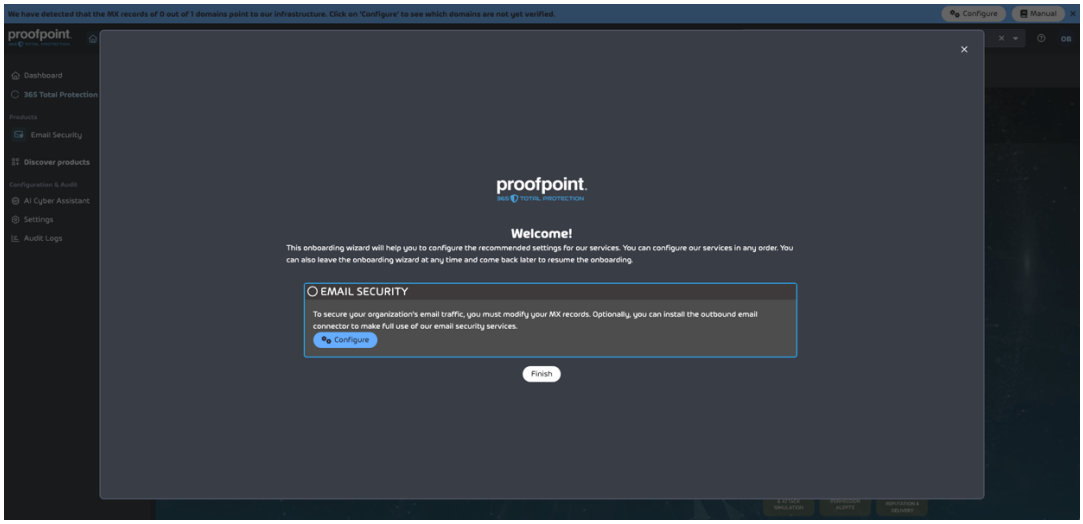
Now that you have completed the additional configuration steps, you can resume the onboarding wizard. Navigate to and click the 365 Total Protection button in the side navigation.



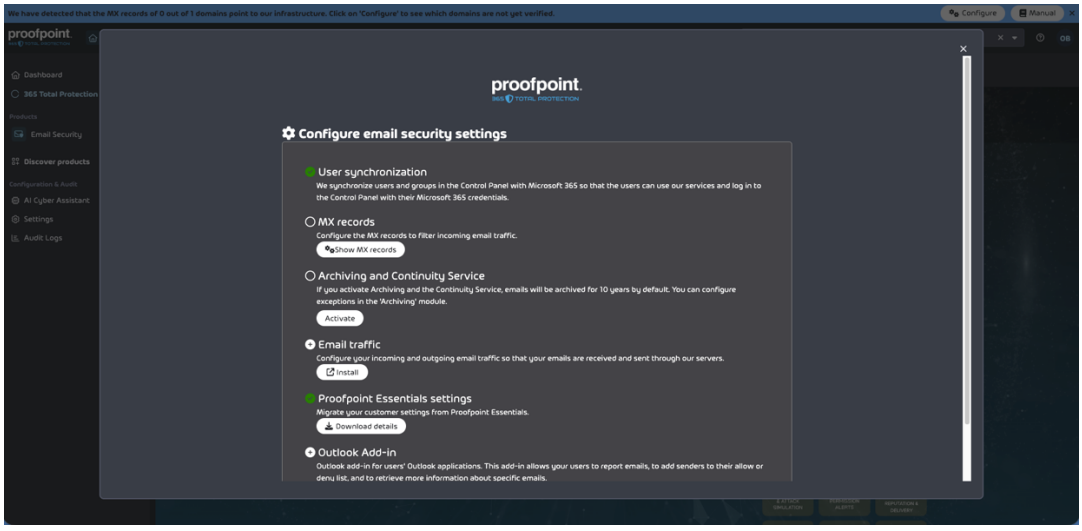
Then click the Resume Onboarding button underneath the Total Protection plan you selected previously.



This will launch the onboarding wizard. Click on the configure button.



You can now proceed with the remaining onboarding steps.



Before you proceed with the additional configuration steps, you should disable any existing Proofpoint Essentials connectors you have in your Microsoft 365 Exchange Admin Center.

Disable the following connectors:

- Outbound Connector for Proofpoint Essentials (US)
- Locked Down – Inbound Connector for Proofpoint Essentials (US).

> ***NOTE**: The connectors may have a slightly different names than what has been indicated. You will want to make sure that you disable the Essentials outbound and locked-down inbound connector before you proceed to the next step.*

Disable Microsoft 365 Spam Filter

To ensure that inbound emails are only processed by Proofpoint Total Protection, we recommend you disable Microsoft 365 Spam Filter settings for traffic originating from Proofpoint IPs. For Proofpoint Essentials partners, you can modify the exisiting rule that is place.

1. Login to Microsoft 365 Admin Center (https://admin.microsoft.com)
2. Click on Exchange under Admin Centers
3. Click on Mail flow, followed by Rules
4. Locate the existing Proofpoint Essentials rule (i.e., "Bypass Spam Filtering for Proofpoint Essentials (US)") and click the rule name
5. Click on Edit rule conditions
6. Click the edit icon (pencil) next to "Sender's IP address in the range
7. For each IP in the table below, copy and paste it into the text field, then click Add.

Total Protection IP Ranges		
83.246.65.0/24	94.100.128.0/24	94.100.129.0/24
94.100.130.0/24	94.100.131.0/24	94.100.132.0/24
94.100.133.0/24	94.100.134.0/24	94.100.135.0/24
94.100.136.0/24	94.100.137.0/24	94.100.138.0/24
94.100.139.0/24	94.100.140.0/24	94.100.141.0/24
94.100.142.0/24	94.100.143.0/24	173.45.18.0/24
185.140.204.0/24	185.140.205.0/24	185.140.206.0/24
185.140.207.0/24		

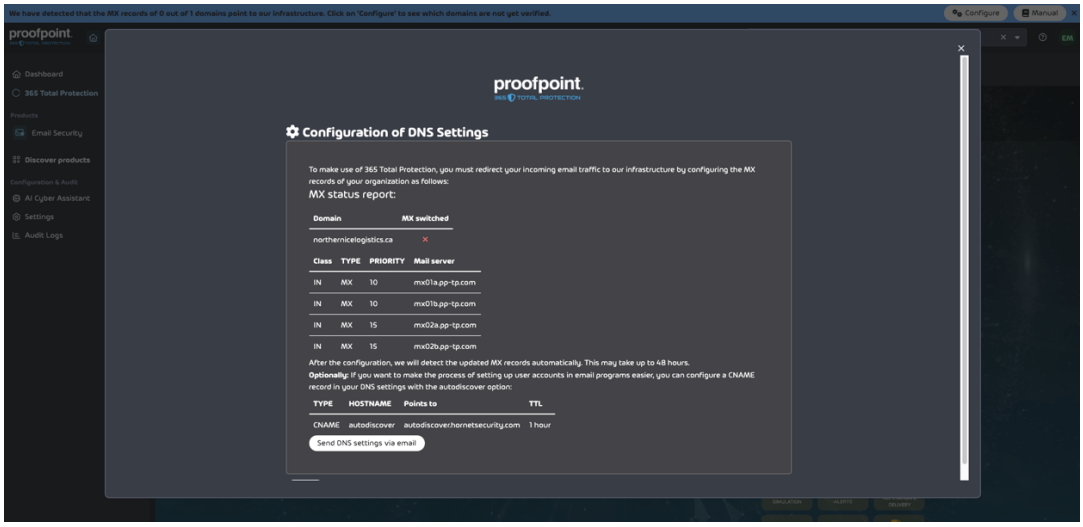
8. Click Save, followed by Save

> ***NOTE**: It can take up to 1 hour for the customer account to be ready to accept mail traffic. We recommend that you do not proceed with the next step until 1 hour has elapsed from the time you initiated the migration.*

MX records

If you are onboarding an on-production domain, we recommend doing this after configuring the rest of options and during a low traffic of email (usually weekends or after-hours) to have the lowest impact possible on email traffic. DNS can take a couple of minutes to update.

Click the Show MX records button.



With this panel open, navigate to your DNS provider and add the following MX records:

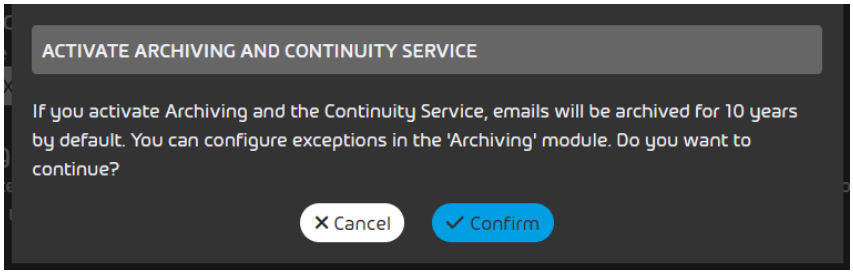
- MX Record 1:
  - Type: MX
  - Priority: 10
  - Value: mx01a.pp-tp.com
  - TTL: 1 hour
- MX Record 2:
  - Type: MX
  - Priority: 10
  - Value: mx01b.pp-tp.com
  - TTL: 1 hour
- MX Record 3:
  - Type: MX
  - Priority: 15
  - Value: mx02a.pp-tp.com
  - TTL: 1 hour
- MX Record 4:
  - Type: MX
  - Priority: 15
  - Value: mx02b.pp-tp.com
  - TTL: 1 hour

***NOTE**: The Proofpoint Essentials MX records can remain in place at this time. However, you will want to reduce thier priority so they are behind the newly added MX records and they should be removed as a final step to complete the migration.*

Archive and Continuity Service (Optional)

This service will archive all inbound and outbound email that passes through Proofpoint's gateways (for archiving internal e-mails a separate journal rule entry will need to be created - https://cp.proofpoint.com/manual/en/365_total_protection/c_enable_archiving_for_internal_mails.html). Also, please note that current e-mails that exist in the Proofpoint Essentials archive will be migrated for partners on the back end at a later data, and you will not be charged on both platforms.

Click the Activate button, followed by Confirm.



You will be able to disable mailboxes or reduce the retention time at a later date. For now, we will only choose to activate the service or not.

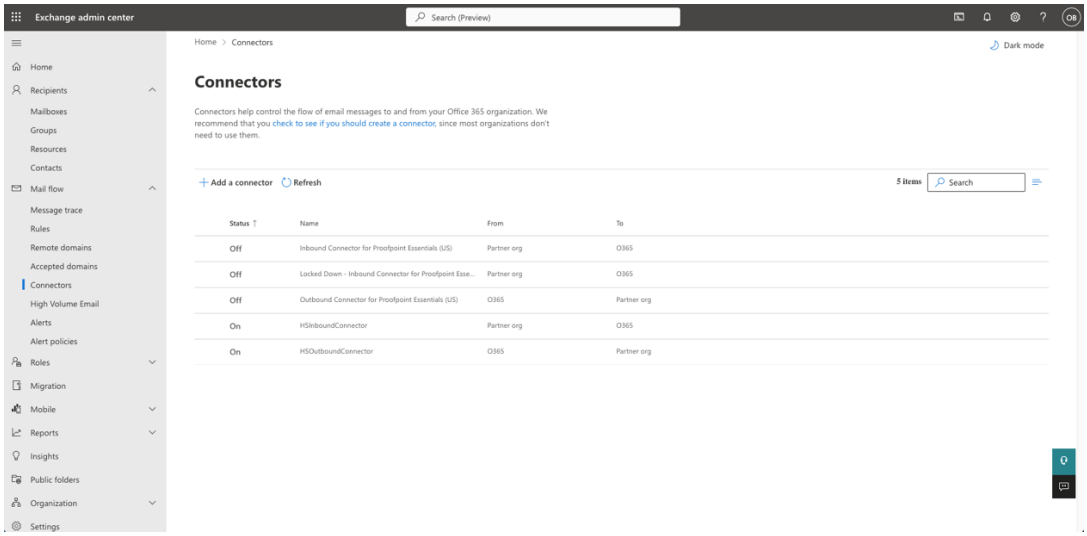
Email Traffic

This step will create the connectors to allow the email flow between Proofpoint and Microsoft environments. This is an automatic process, and by just clicking install, we will do everything for you.

Click the Install button underneath Email Traffic to create the connectors. This will require that you authenticate with the Microsoft 365 tenant with the same Global Admin account used earlier and will request you accept additional permission changes.

When this has been completed, you will see a green checkmark next to the Email Traffic step and the Install button will be disabled. You can also login to the Exchange Admin Center and you will see the new connectors.

> ***NOTE**: Your previous Essentials connectors were disabled in a previous step.*



Outlook Add-In (Optional)

If you wish to install the Proofpoint 365 Total Protection Add-in for Outlook, you can do so at this step. This Add-in will allow user to add senders to a allow or deny list, report an email as malicious and more.

To install the add-in, click on the Install button under the Outlook Add-In section. This step will also require that you grant additional Microoft365 permissions. Over the next hours all users will see the add-in in their Outlook app and the web-based Outlook client.

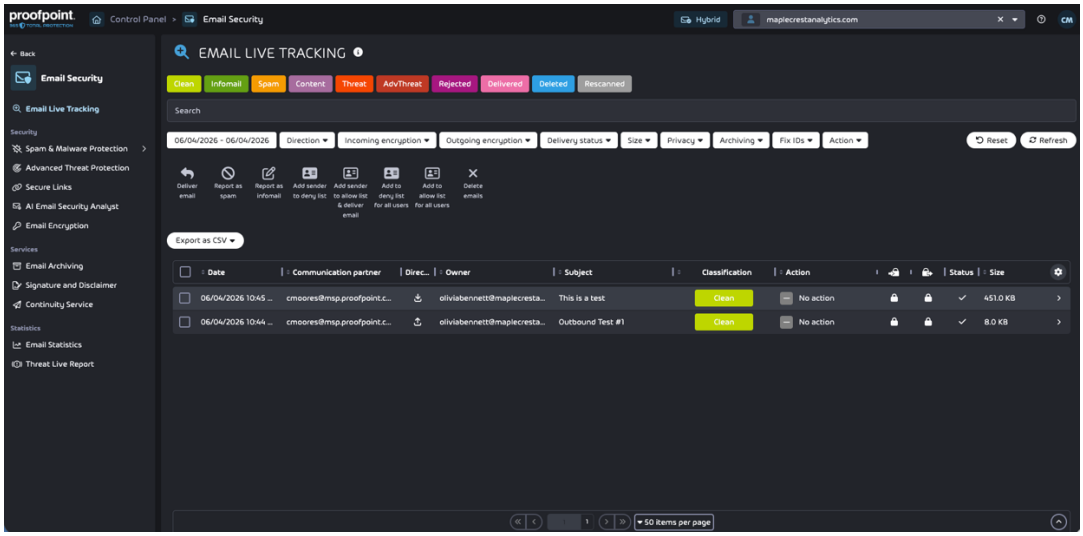
Once all the Configuration Steps have been completed, you can close the window by clicking on the X button in the top right-hand corner.

Verify Mail Routing

To verify mail routing, you should navigate to Email Live Tracking (equivalent to Proofpoint Essentials Email Logs). From the left side navigation, click on Email Security, followed by Email Live Tracking. You should immediately see both results appear that show inbound and outbound traffic.

You can also test deliver by sending a test email from the customer's environment to an external mailbox. After you hit send, refresh the Email Live Tracking screen to see the logged result.

In addition, send a test email to the customer's environment from an external mailbox. After you hit send, refresh the Email Live Tracking screen to see the logged result.



Once you have verified email routing, you should **remove the legacy Proofpoint Essentials MX records** and **remove the Proofpoint Essentials portion of the SPF record**. The legacy connectors that were previously disabled can also be removed. Otherwise, traffic may still be routed through the Essentials account.

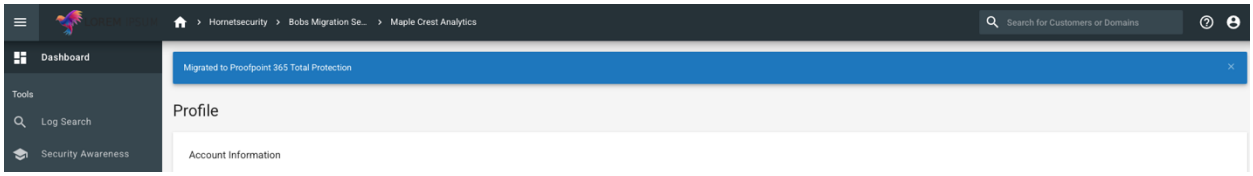
Proofpoint Essentials Access

You will continue to have access to Proofpoint Essentials.

For customers on all packages other than Professional/Professional+, access will be available for a minimum of 30 days.

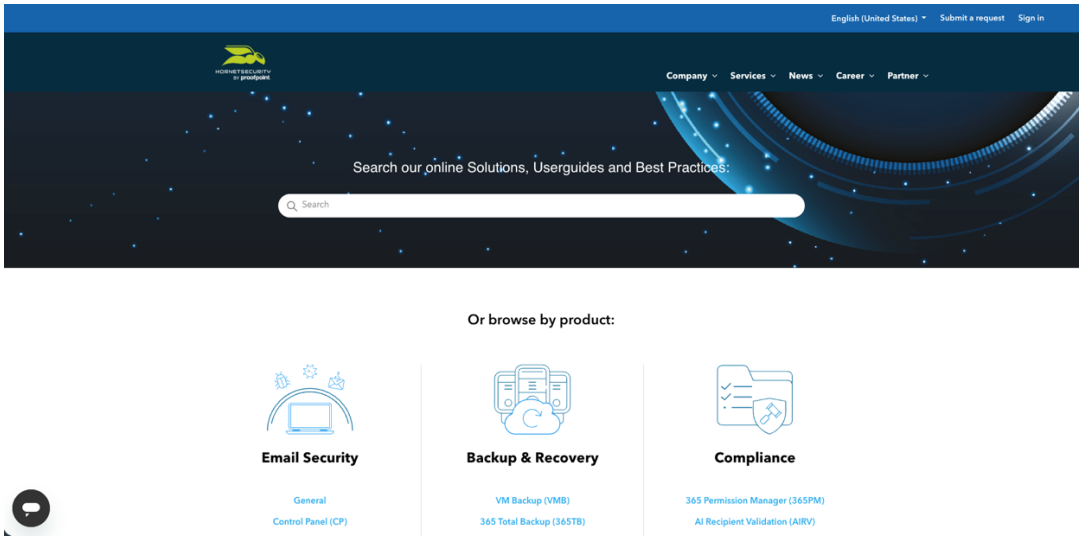
For customers on Professional/Professional + packages that include archiving, access will be available until the customer's archive has been migrated to Proofpoint 365 Total Protection.

When you log into the customer's Proofpoint Essentials account, you will see a newly added banner to the console.

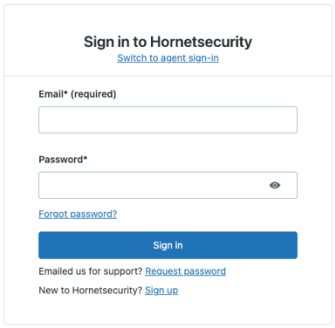


Accessing Support

You can contact our Support team by accessing https://support.hornetsecurity.com



Click on the Sign in option in the toolbar. If you have not registered with support, Click the sign-up link next to “New to Hornetsecurity?”.



In addition, please refer to https://www.proofpoint-total-protection.com/essentials-migration/ for additional information related to the Essentials migration tool and process.