proofpoint.

Microsoft 365 Integration Guide

Proofpoint Essentials integration with Microsoft 365

Product Version:.5.20230914+

Deployment Type: Proofpoint Essentials + Microsoft 365 Online

Document Owner: Proofpoint Essentials Product Management

Document Version: 0.01

Last Updated: 16th October 2023.

proofpoint.

Table of Contents

Document Introduction

This document identifies best practices when integrating Microsoft 365 with Proofpoint Essentials. Please review this entire document before making changes to Proofpoint Essentials, Microsoft 365, or DNS.

Proofpoint's standard configuration best practices are recommended for all Proofpoint customers to ensure the full benefit of Proofpoint solutions purchased are received.

Overview

Proofpoint Essentials can be configured as the inbound mail gateway through which all incoming mail for specified domains is filtered before reaching Microsoft 365.

It can also be configured as the outbound mail gateway through which all mail sent from a Microsoft 365 tenant to an external recipient can be filtered. Utilising this configuration, the Microsoft 365 mail servers will pass outgoing mail through the Proofpoint Essentials to be filtered before final delivery.

The Microsoft 365 Integration automates several of the steps necessary to configure Proofpoint Essentials as an inbound and outbound mail gateway. After running the Microsoft 365 Integration onboarding of your Microsoft 365 tenant to Essentials, and prerequisite mail flow configuration will be complete. The following configurations are made automatically

- The Proofpoint Essentials M365 integration Azure application, will be granted access necessary to make the configurations
- Essentials will import domains from Azure and provide default configuration necessary to enable mail flow. **Note: domains will not be enabled for mail relay. Enabling of these entities will need to be carried out manually by your organization's Essentials admin.**
- Essentials will configure Azure Directory Sync, **Note: First time sync and recurring schedule will need to be carried out manually by an admin.**
- The Proofpoint Essentials M365 Azure application will configure mail flow rules and connectors in your organizations Exchange Online. **Note: the outbound connector will be disabled by default. It should not be enabled until your organization has performed a DNS change to include Proofpoint Essentials in your SPF record. Enabling this connector will need to be carried out manually by your organization's Microsoft 365 admin.**

CAUTION: Proofpoint recommends any changes in the Proofpoint Essentials, DNS, or Microsoft 365 take place during a well-planned change control window to help reduce the risk to your organization.

Impact in Microsoft 365

As part of the Microsoft 365 integration process, Proofpoint Essentials will configure several entities in Microsoft 365. The necessity for these entities is described in this section.

Azure

Security Principle

The Proofpoint Essentials M365 Application will be installed in your organizations Azure tenant as a security principle. Your organization's Azure admin will be able to view and manage the new security principle within Azure. Further information can be found here: https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/view-applications-portal

Note: it is possible for your organization's Azure admin to modify the installed security principle in such a way that the connection with Proofpoint Essentials will lose it's connection. Please be aware of this risk before making changes.

Exchange Online

The Proofpoint Essentials M365 Application will create 'Connectors' and 'Rules' in your organizations Exchange Online service.

Note: The outbound connector is disabled by default and need to be updated after you have configured your organization's DNS to include Proofpoint Essentials in your SPF record.

Connectors

Inbound Connector for Proofpoint Essentials

This connector will relay inbound mail traffic to Essentials (providing to the customer any email security features enabled in Essentials). It will utilize the rule described in the section below.

Outbound Connector for Proofpoint Essentials

This connector relays outbound mail traffic to Essentials (providing to the customer any email security features enabled in Essentials).

Rules

Bypass Spam Filtering for Proofpoint Essentials

This rule is used to ensure that your organization's Exchange Online service does not treat any of Proofpoint Essential's IP addresses as a spam source.
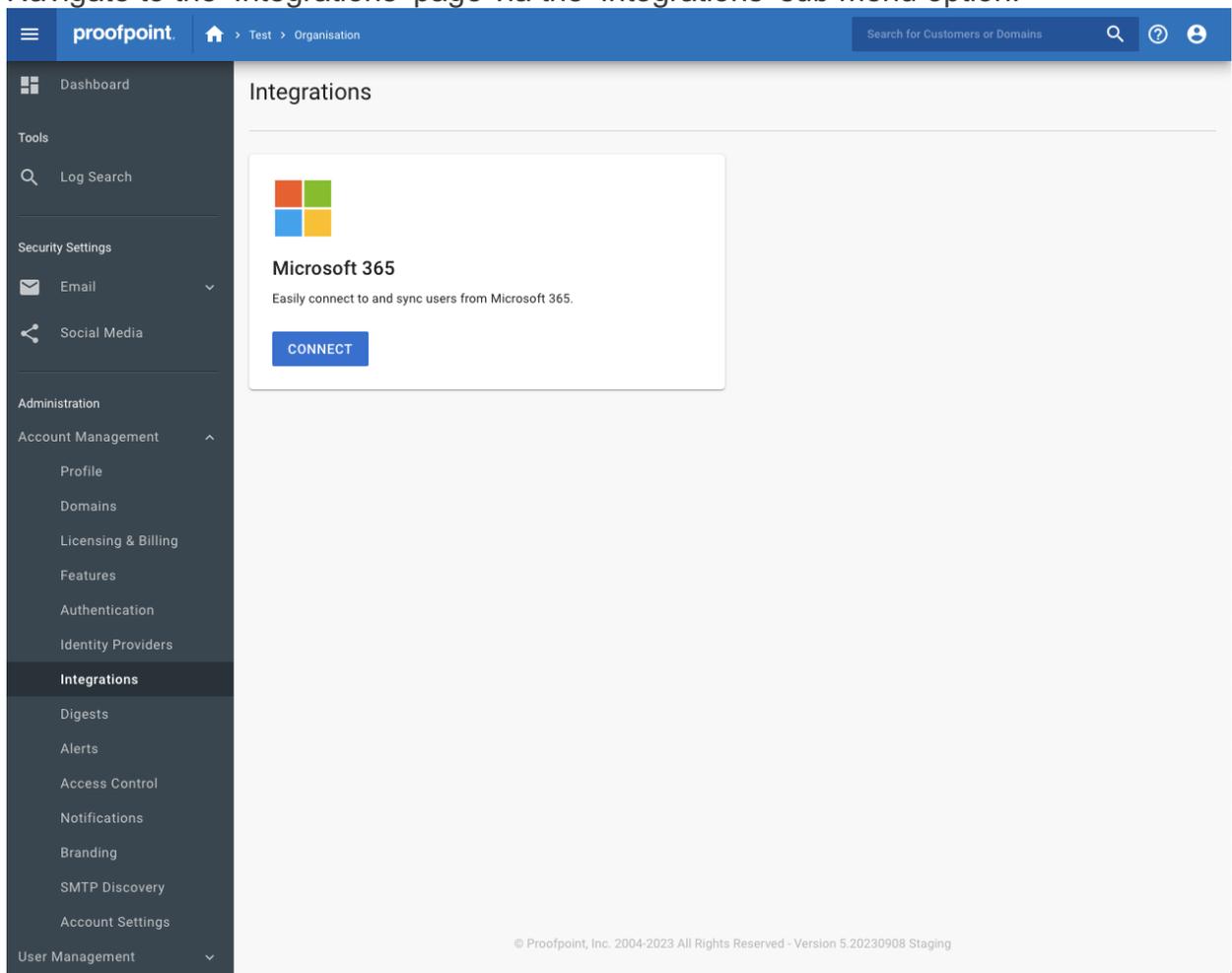
Microsoft 365 Integration Usage

Feature Enablement

Please contact your Proofpoint Essentials representative to have this feature added to your current package entitlement if it does not appear under Integrations.

Running Microsoft 365 Integration for your organization

Once the feature has been enabled your organization's Proofpoint Essentials admin can perform the Microsoft 365 Integration by following these steps:

1. Login to the Proofpoint Essentials web portal.
2. Expand the 'Account Management' option in the side menu.
3. Navigate to the 'Integrations' page via the 'Integrations' sub menu option.

4. Click the 'CONNECT' button.

5. Review the details regarding the Proofpoint Essentials features which will be configured automatically. If they are acceptable, click the 'NEXT' button.

6. A new browser window will pop up, prompting you to login to your Microsoft Online account. Enter credentials which provide 'Global Admin' permissions to your target Microsoft 365 tenant.
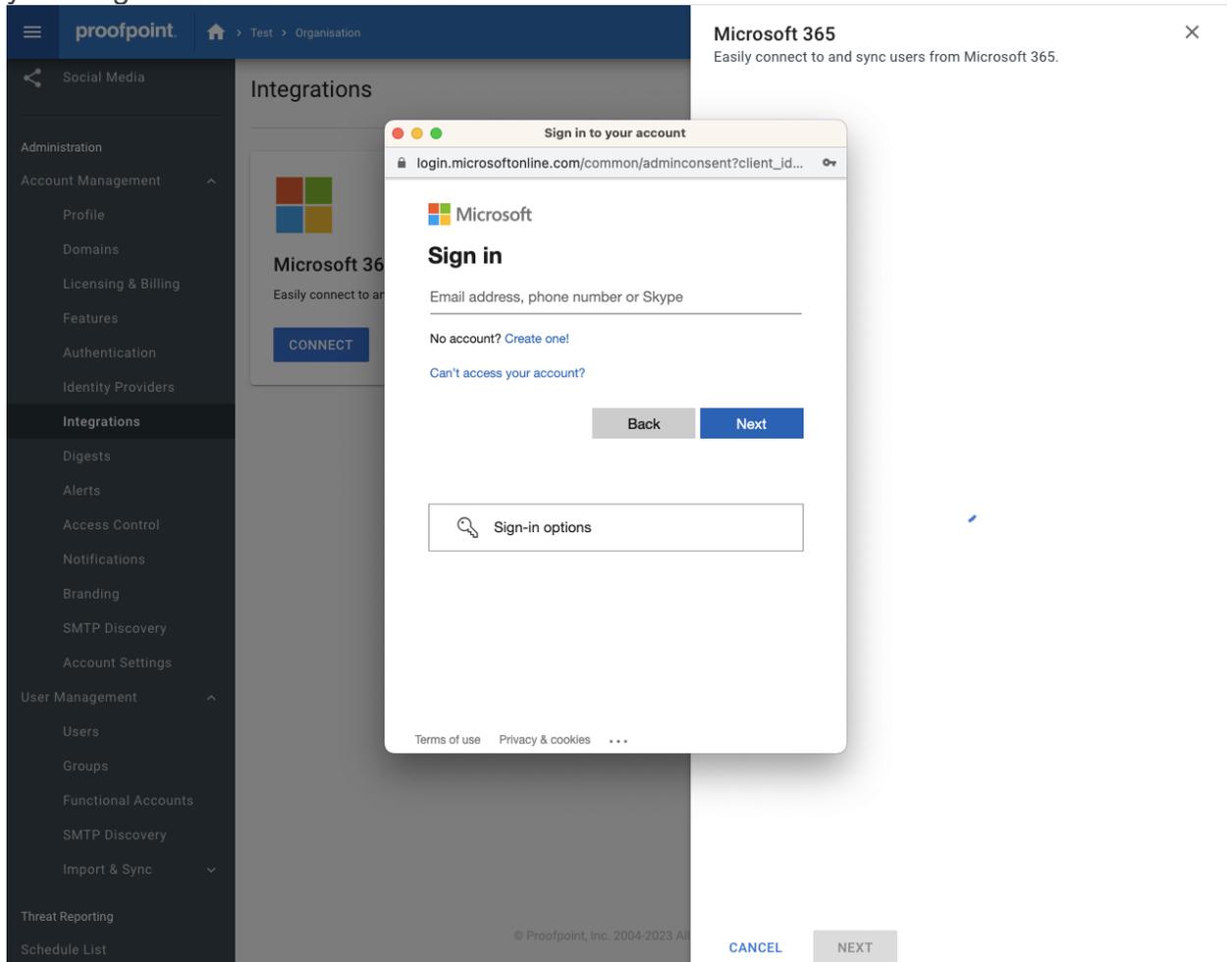
7. Click the 'Next' button.

8. Review the permissions requested by the Proofpoint Essentials M365 Application. The necessity for these permissions is described in the 'Application Permissions' section later in this document. If they are acceptable, click 'Accept' to start the Microsoft 365 Integration automation.
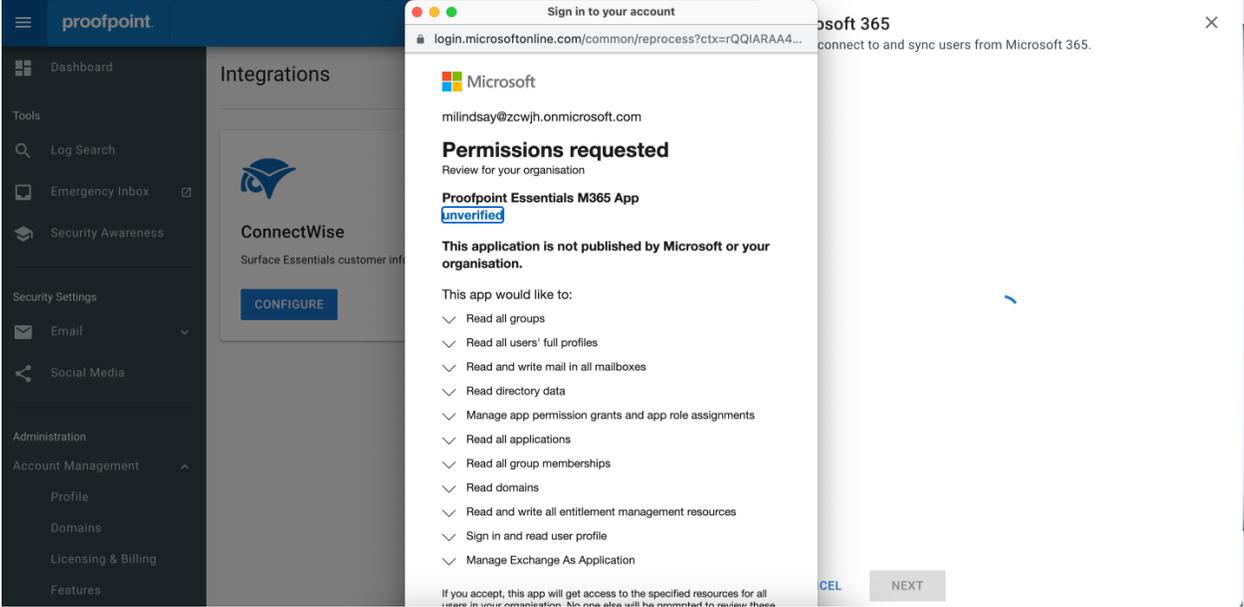
The automated process will begin and may take a few minutes to complete.

Enabling Microsoft 365 Integration for your child organizations

Once the feature has been enabled your organization's Proofpoint Essentials admin can enable the feature for child organizations.

1. Login to the Proofpoint Essentials web portal.
2. Expand the 'Customer Management' option in the side menu.
3. Navigate to the 'Automation Settings' page by clicking the 'Automation Settings' sub menu option.
4. Under the 'Integrations' section in the 'Automation Settings' page, click the checkbox labelled "Allow customers to use integrations".

This will expose the "Integrations" side menu option and the Microsoft 365 Integration options to all of your organizations children organizations.

Microsoft 365 Integration Application Permissions

During the Microsoft 365 setup process, the admin is redirected to a Microsoft Online login. This is referred to by Microsoft as an "Admin Consent Flow".

The Azure admin consent flow is a mechanism used to grant permissions to an Azure Active Directory application by an administrator. It allows an application to request permissions that require admin consent, and provides the admin the opertunity to review and approve these permissions on behalf of their organization.

For further information consult Microsoft Documentation:

https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/admin-consent-workflow-overview

The specific list of permissions that the Proofpoint Essentials M365 application needs, in order to perform automation of mail flow configuration, is listed below with an explaination of the necessity for each. **Note: some automation tasks require multiple permissions.**

Application.Read.All
Used to perform self-management (of the Proofpoint Essentials M365 application) and facilitate Exchange Online mail flow configuration.

AppRoleAssignment.ReadWrite.All
Used to self-assign the Exchange Online management role in order to create the rules and connectors necessary for mail flow.

Domain.Read.All
Used to import domains for the purpose for configuring mail flow in Proofpoint Essentials.

Used to import domains for the puspose of determining users to sync via Azure Directory Sync.

EntitlementManagement.ReadWrite.All
Used to self-assign the Exchange Online management role in order to create the rules and connectors necessary for mail flow.

Exchange.ManageAsApp
Used to enable Exchange Online management for the application in order to create the rules and connectors necessary for mail flow.

Group.Read.All
Used by Azure Directory Sync to import organization groups into Essentials.

GroupMember.Read.All
Used by Azure Directory Sync to recreate groups during import of users into Essentials

Mail.ReadWrite

Used by 'One Click Remediation' feature to enable Proofpoint Essentials to manage mail disposition directly in a user's inbox i.e move a mail to/from quarantine.

RoleManagement.ReadWrite.Directory

Used to enable Exchange Online management for the application in order to create the rules and connectors necessary for mail flow.

User.Read.All

Used by Azure Directory Sync to import organization users into Essentials.

12 of 12