ManageEngine
M365 Manager Plus

The definitive Microsoft 365 compliance and security guide

Table of contents

1. Introduction

As an IT administrator, your biggest concerns are keeping your organization secure and meeting compliance requirements. But what are security and compliance? Let's start by taking a deeper look at each of these terms and how they differ from each other.

Security is the practice of protecting the integrity and confidentiality of the critical business information and assets in your possession. Compliance, on the other hand, involves taking steps to ensure your digital resources are protected, and is mainly the process of adhering to the requirements set by third parties, including government regulations, terms of a contract, and security frameworks. In short, compliance is a measure adopted to prove that your network is secured.

A common misconception among organizations is that if their setup is compliant, it also means that they're secure. We've seen organizations such as Home Depot and Target suffer huge data breaches despite being PCI-compliant. So what should organizations focus on instead to ensure security?

The main focus for any business is to protect the confidential data in its possession, as any loss of data can destroy an organization's reputation, leading to huge costs in damages. To protect confidential data, both compliance and security are equally important. Every organization needs to combine a strong security program with a compliance plan to reduce the risk of data breaches.

M365 Manager Plus is an extensive Microsoft 365 tool that helps you comply with various IT compliance mandates as well as mitigate any security threats looming over your Microsoft 365 setup.

2. M365 Manager Plus: Your Microsoft 365 compliance and security management tool

M365 Manager Plus is a comprehensive Microsoft 365 reporting, auditing, monitoring, management, and alerting tool. Its user-friendly interface makes it easy to manage Microsoft 365 services such as Exchange Online, Azure Active Directory, Skype for Business, OneDrive for Business, and Microsoft Teams, all from a central console (Figure 1).

M365 Manager Plus provides over 700 preconfigured reports that consolidate data from your Microsoft 365 components, giving you complete visibility into your Microsoft 365 setup. You can monitor Microsoft 365 services around the clock, and receive instant email notifications about service outages. It also eases compliance management with built-in compliance reports, and offers advanced auditing and alerting features to keep your Microsoft 365 setup secure.

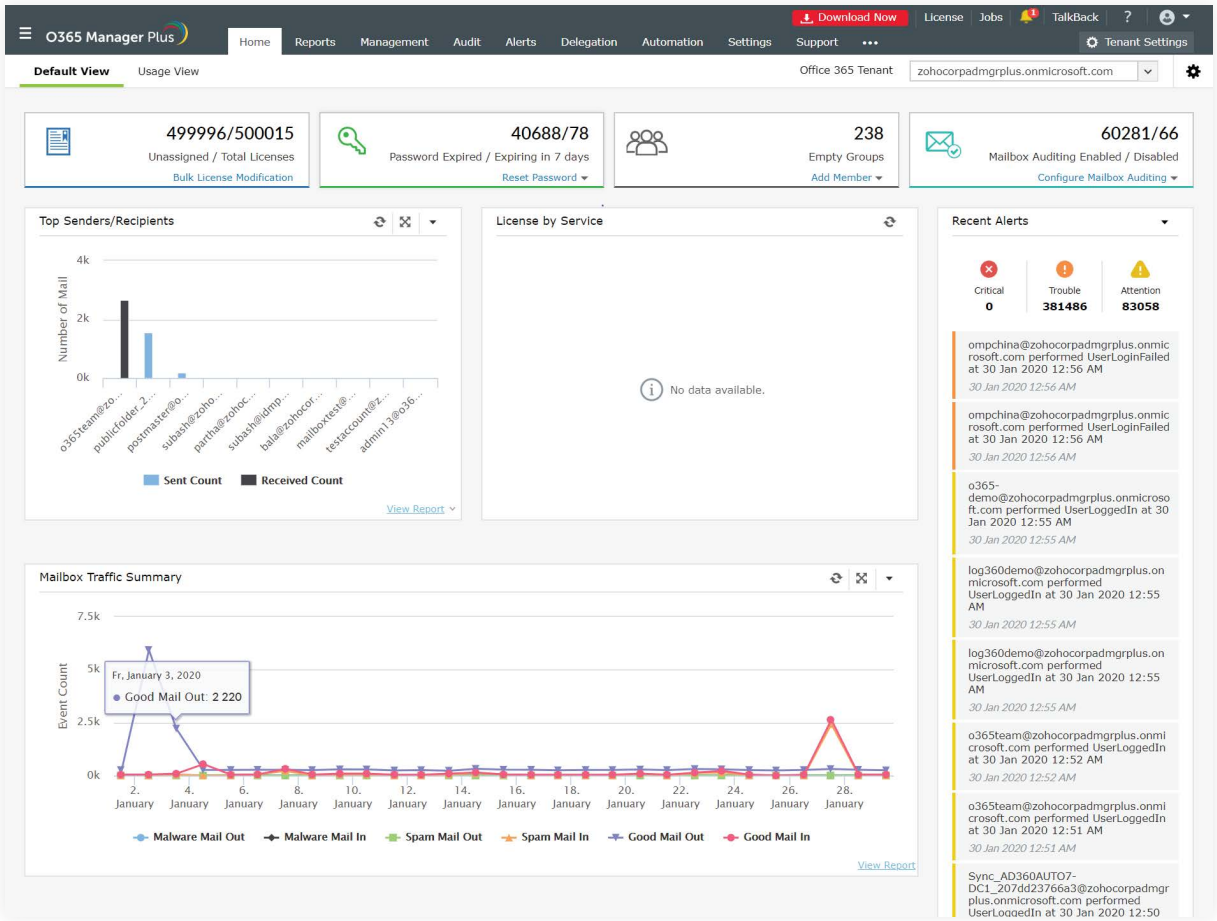


Figure 1. M365 Manager Plus' dashboard.

3. Compliance is a click away with M365 Manager Plus

Organizations have to implement various control methods to comply with different industry mandates. M365 Manager Plus keeps tabs on all user and admin activities in your Microsoft 365 environment, so you can comply with regulatory mandates such as SOX, HIPAA, PCI DSS, GLBA, and FISMA. For detailed compliance reporting, we have compiled checklists of the required control methods for some of the most important compliance mandates.

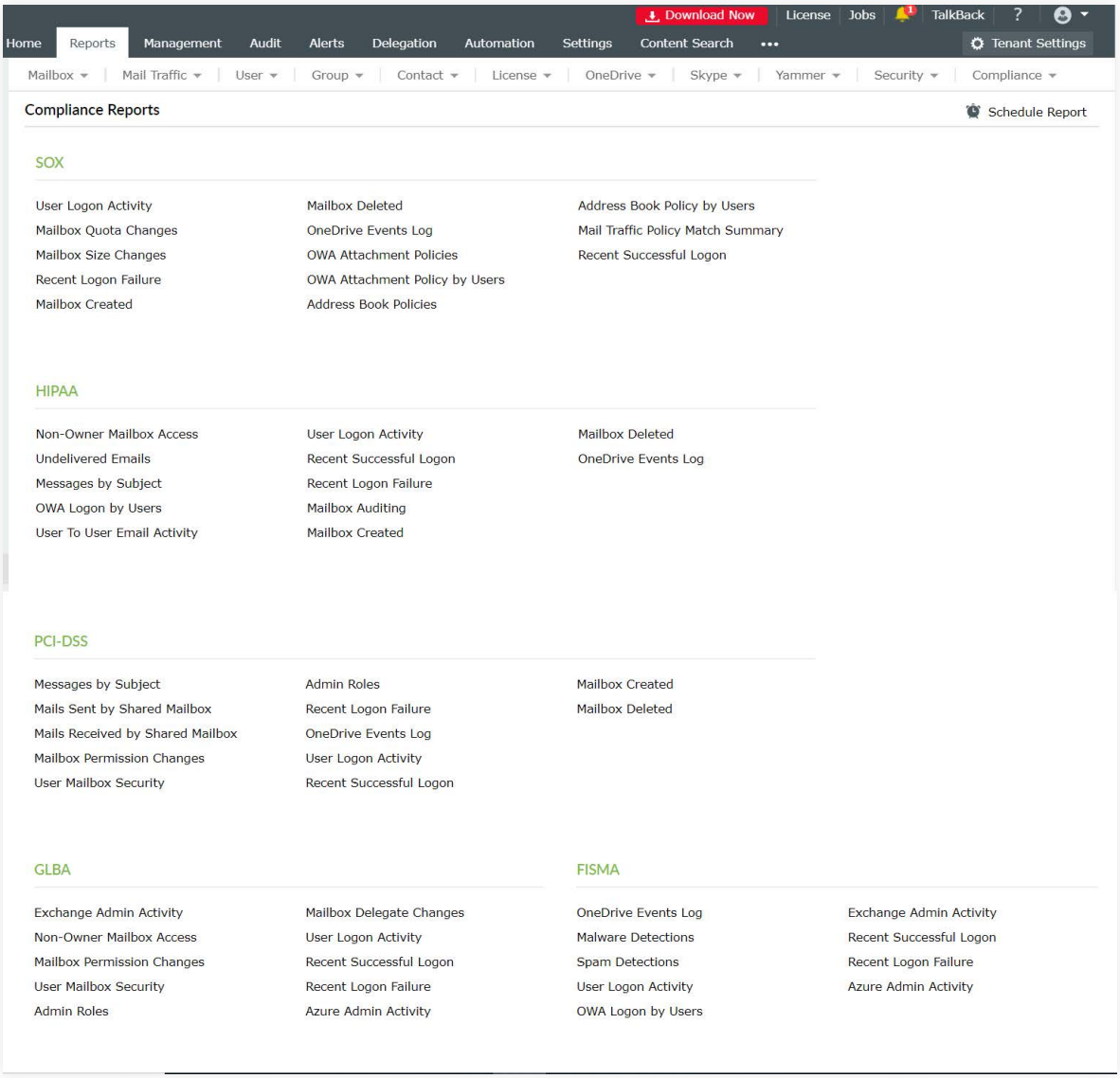
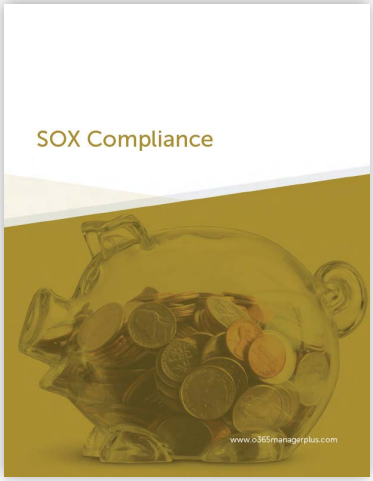


Figure 2. Prebuilt compliance reports mapped to their respective compliance regulations.

3.1 Checklists

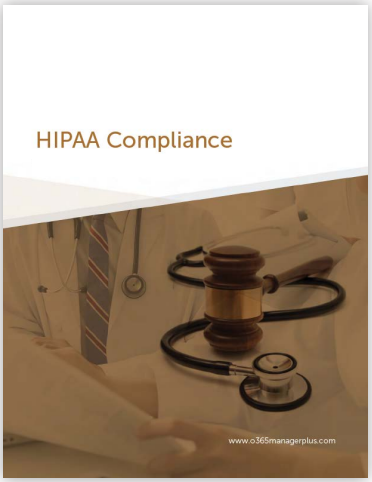
Using M365 Manager Plus' compliance reports, you can keep your organization's information safe and meet the requirements of various compliance standards.



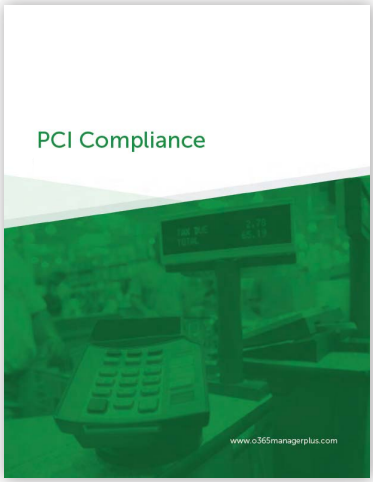
Download SOX compliance checklist

Download FISMA compliance checklist

Download GLBA compliance checklist



Download HIPAA compliance checklist



Download PCI DSS compliance checklist

Note: The procedures for establishing compliance may vary depending on your systems configuration, internal procedures, the nature of your business, and other factors.

4. Overcoming security challenges with M365 Manager Plus

M365 Manager Plus offers a wide array of features to ensure the security of your Microsoft 365 environment.

4.1 Detecting spam and malware

M365 Manager Plus provides the following capabilities to detect spam and malware in your Microsoft 365 setup:

- Comprehensive monitoring of all inbound and outbound traffic in your Exchange Online environment.
- Custom summary audit views for faster threat detection.
- Scheduled reports for all spam and malware information for regular security audits.
- Alert notifications that help with early detection.

4.1.1 Auditing

M365 Manager Plus detects spam and malware in emails and provides detailed information such as sender, subject, and recipient, as shown in Figure 3.

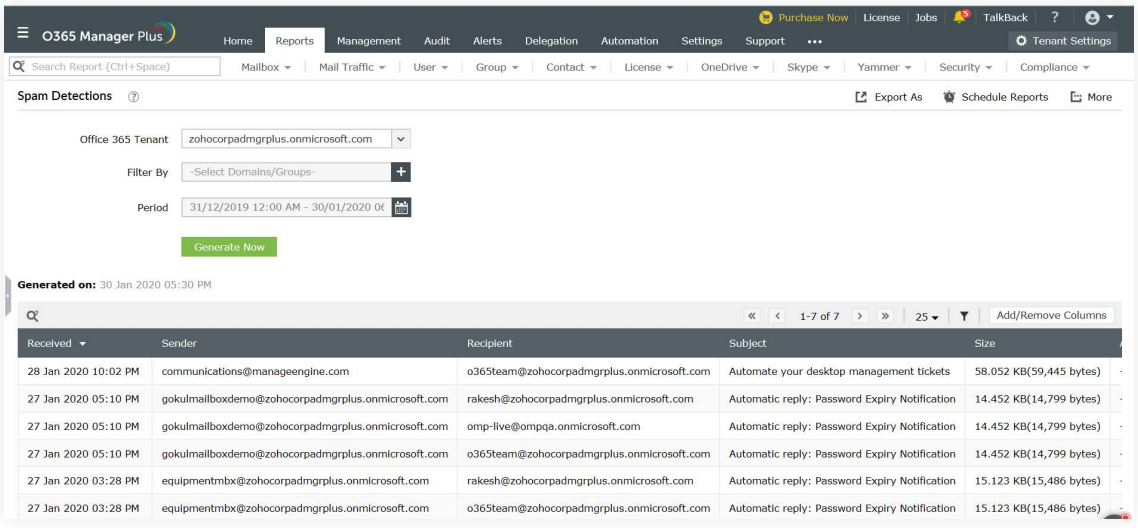


Figure 3. M365 Manager Plus spam detection.

4.1.2 Creating custom views

Using M365 Manager Plus you can set custom views for audit summaries based on spam/malware sender address, spam/malware recipient address, domain, and more, as shown in Figure 4. These custom views make monitoring quicker and more convenient.

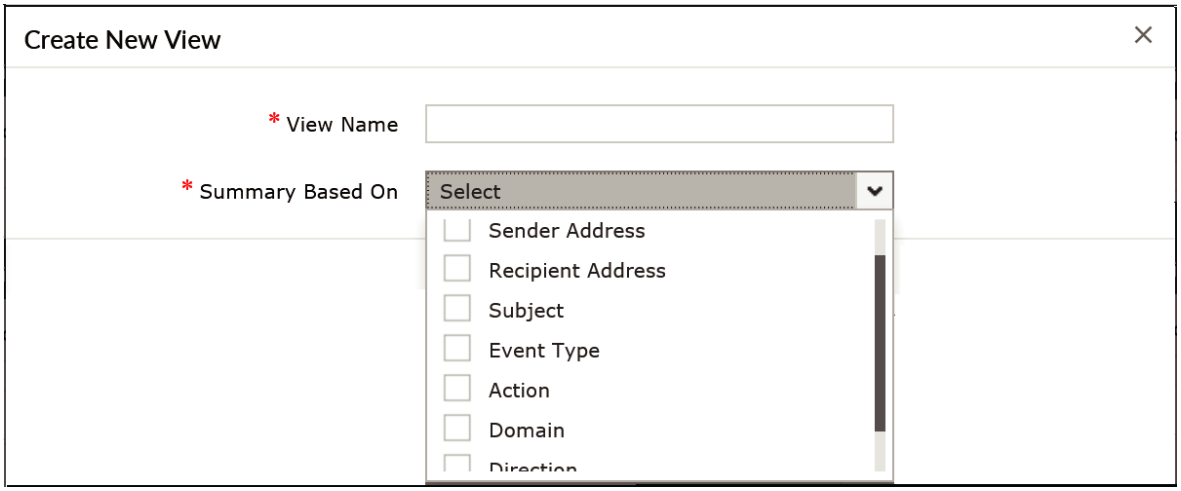
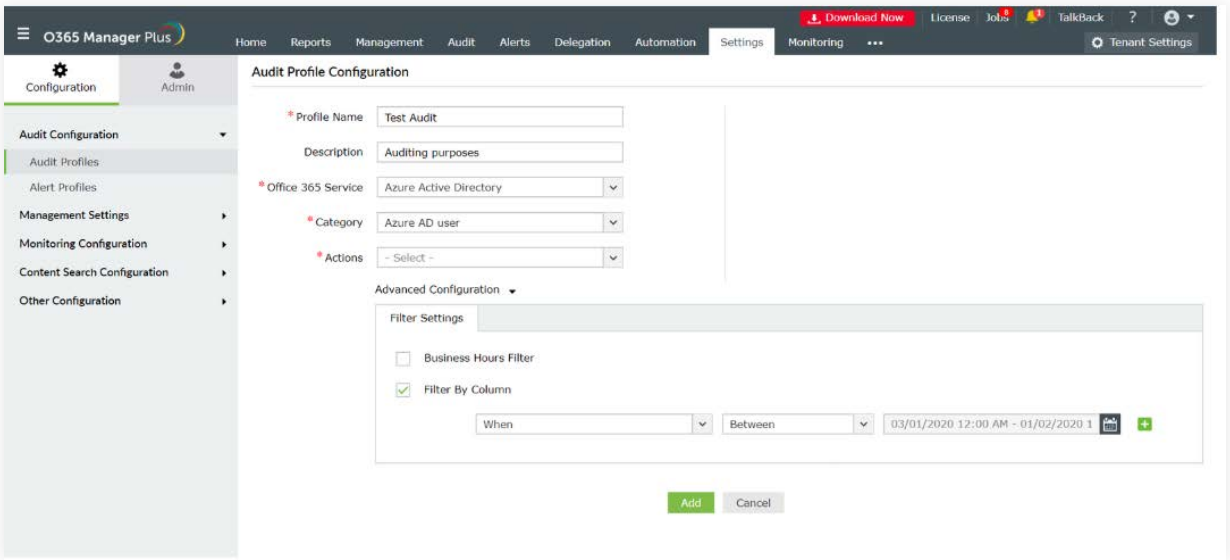


Figure 4. Creating a custom spam and malware detection summary view.

4.1.3 Advanced audit filters

You can use the filters available under the audit profile configuration option to scrutinize your preferences further.

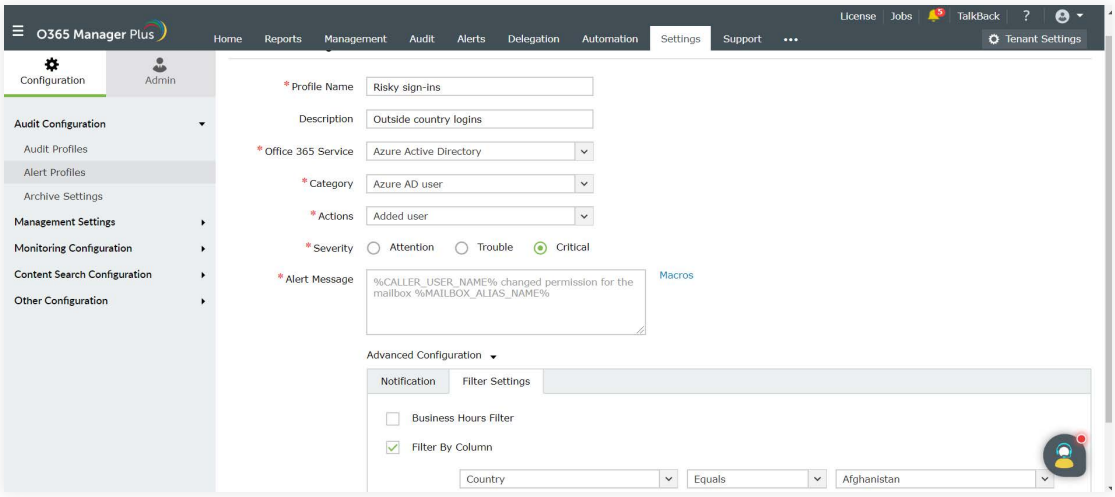


4.1.4 Geo-location

In M365 Manager Plus, Geolocation option has been enabled for audit reports and alert triggers. Using this option you can find out the country from where a user is performing a specific operation, by tracking the IP address of the device. The operations covered under this geolocation tag include user login process, changing account password and so on.

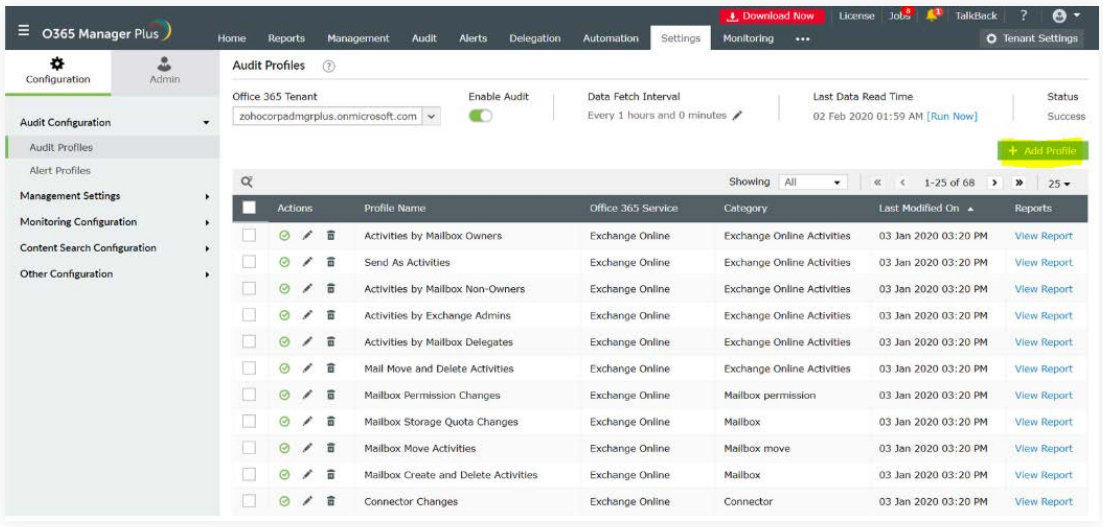
Using this feature of M365 Manager Plus it is now very easy to maintain track over the user's actions. You can use this feature along with the Business hours settings available in the product to monitor the sign-ins. You can put to use the geolocation functionality available with the audit reports by choosing the Add/Remove columns option.

You may also use filters for alert profiles like the Client IPs filter, to find out the activities done outside the organization network or your trusted IP ranges. You may also choose to block or trust IPs based on the data you get.



4.1.5 Customized audit profiles

You can create your own profiles for auditing using the Add profile option available under the audit tab.



4.1.6 Alerting

M365 Manager Plus can send notification messages to admins containing details about the spam/malware sender's email address, recipient's email address, subject of the spam email, and more, as shown in Figure 5. With this information, you can take immediate action after discovering an attack.

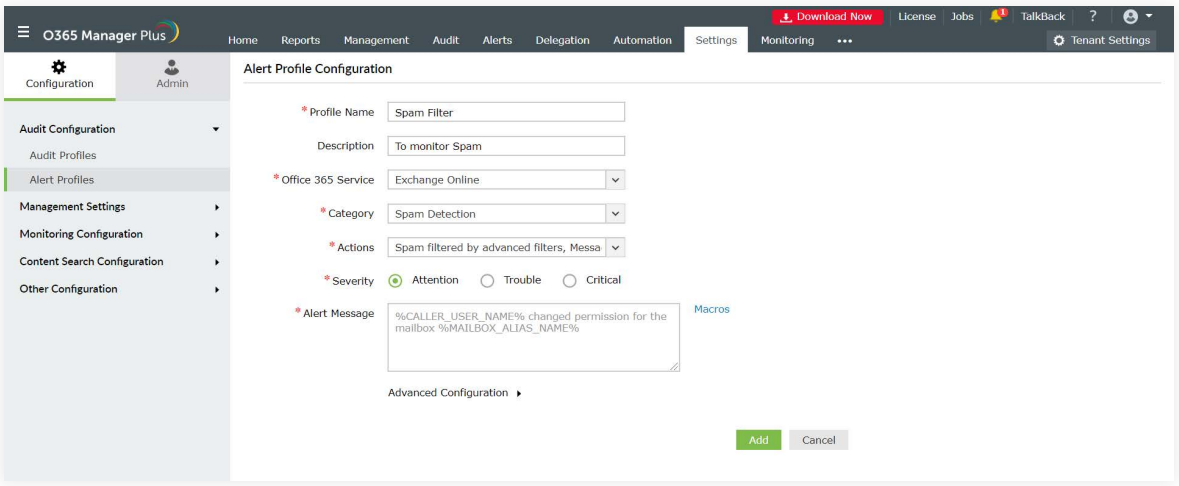


Figure 5. Spam alerts.

4.1.7 Reporting

Using M365 Manager Plus, you can generate various reports on spam and malware in emails, including:

- Top Spam Recipients
- Top Malware Recipients
- Malware Detections
- Spam Detections

4.2 Monitoring DLP policy matches

M365 Manager Plus helps prevent data loss via email by monitoring and investigating email traffic. It helps you:

- Gather information from the data loss prevention (DLP) policy matches report, or set DLP policy match alerts to prevent sensitive information from being compromised.
- Filter the DLP policy matches based on time, sender, recipient, and more to better understand the trends and reasons for data loss.

4.2.1 Auditing and alerting

One way M365 Manager Plus detects data loss is by identifying emails that match DLP policies. If an email contains data matching the policy, M365 Manager Plus provides all details about the email, including the sender, recipient, subject, domain information, and the DLP policy that's matched to it.

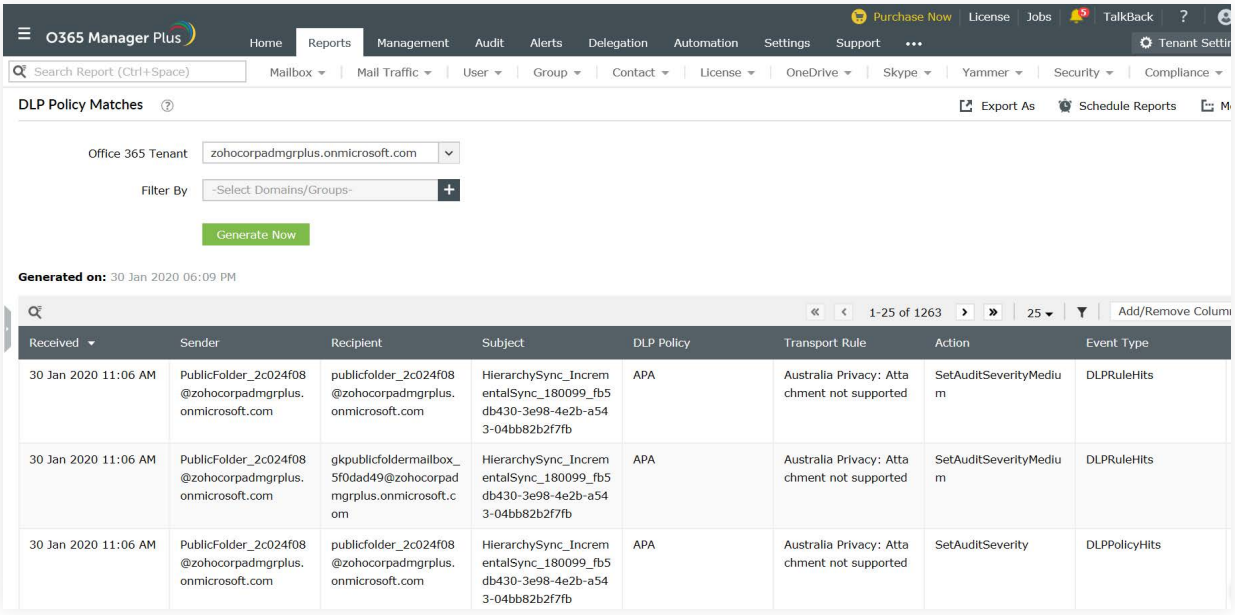


Figure 6. Auditing DLP policy matches.

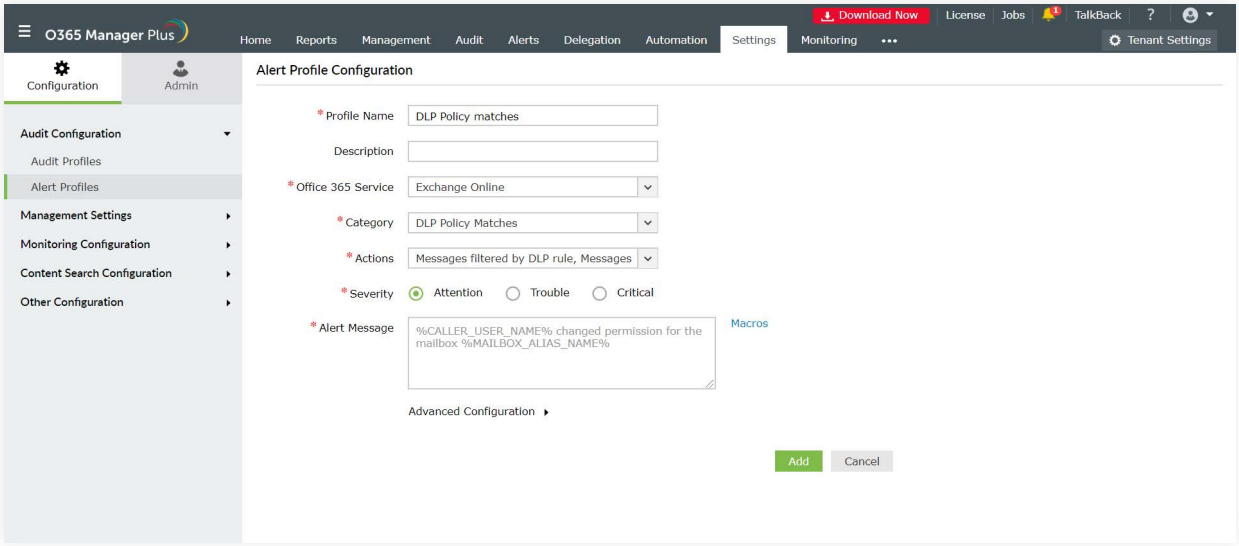


Figure 7. DLP policy match alert configuration.

5. Microsoft 365 security reports

M365 Manager Plus provides the following categories of reports to comprehensively monitor and strengthen the security of your Microsoft 365 environment:

- Activity reports
- User and mailbox security reports

M365 Manager Plus also helps you comply with the stringent requirements of IT compliance regulatory mandates like PCI DSS (requirement 10.2.2 and 11.5), ISO 27000 (requirement A.12.4.3), SOX (section 404), HIPAA (section 164.308 (a)(1)(ii)(D)), and FISMA (NIST SP800-53), by keeping tabs on all administrator and user activities in your Microsoft 365 environment.

5.1 Activity reports

Most organizations delegate administrative responsibilities among different admins and sometimes need to elevate a user's rights. Activity reports let you know when admins, users with elevated rights, or any other users make critical changes in your Microsoft 365 environment, so you can easily identify unauthorized modifications.

5.1.1 Admin Activities

Get a comprehensive overview of all administrator activity in your Microsoft 365 environment with reports on:

- Exchange Admin Activity
- Azure Admin Activity
- Hold activity

5.1.1(a) Exchange Admin Activity

This report provides an overview of all administrators' activities in your Exchange Online environment, such as what activity was performed, who performed the activity, the status of the operation, and which objects were modified.

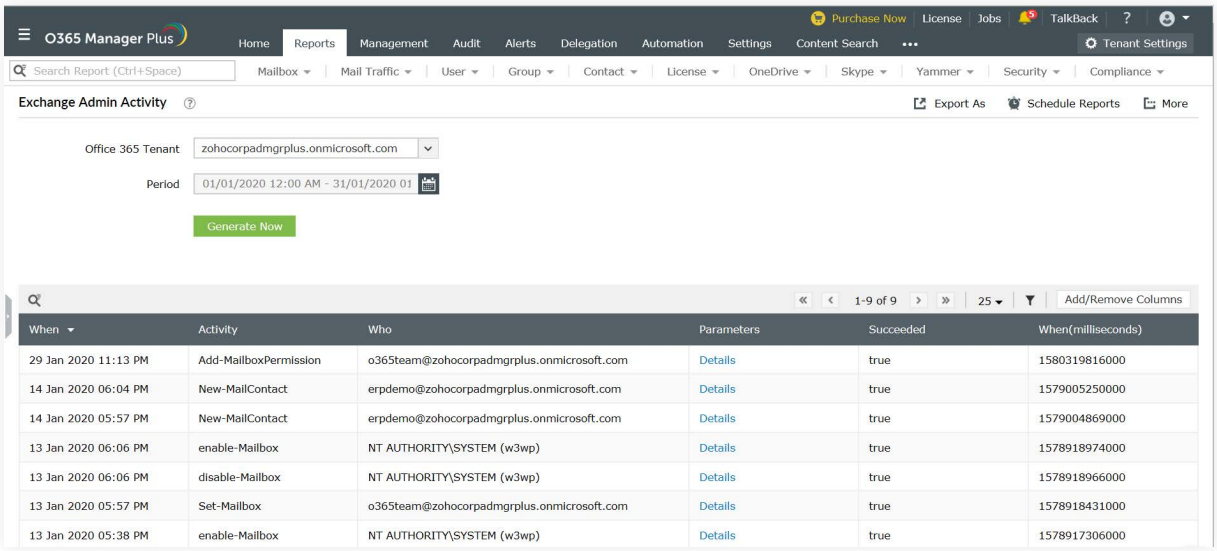


Figure 8. Exchange Admin Activity report.

5.1.1(b) Azure Admin Activity

This report helps you monitor, audit, and report on Azure administrators' activities, and ensure the integrity and security of your organization's Azure environment.

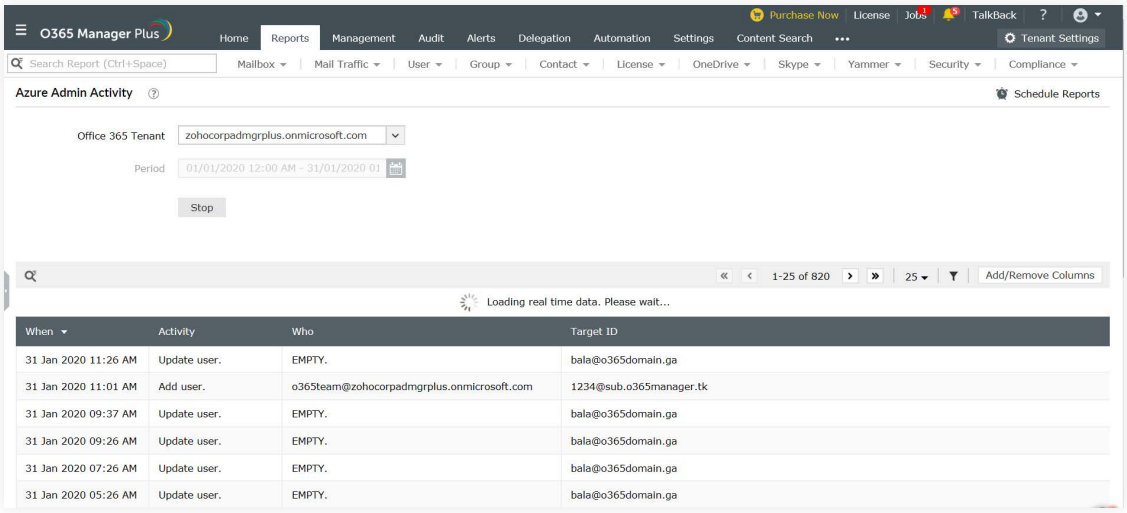


Figure 9. Azure Admin Activity report.

5.1.1(c) Hold activity reports

Placing a hold on a mailbox retains emails for either a specific period of time or indefinitely. This ensures that all emails are retained and left unaltered for legal purposes. Any alteration can cause huge legal ramifications, so it's important to closely monitor every change made to hold objects. M365 Manager Plus' hold activity reports provide details on all changes made to InPlace Hold and Litigation Hold objects, including information on the change, the person responsible for the change, the parameters changed, and the status of the change.

5.1.1(c)(i) Litigation Hold Activity

This report provides details on all changes made to the Litigation Hold on mailboxes, as shown in Figure 10. These details include what object was modified, what activity was performed, and who made the change.

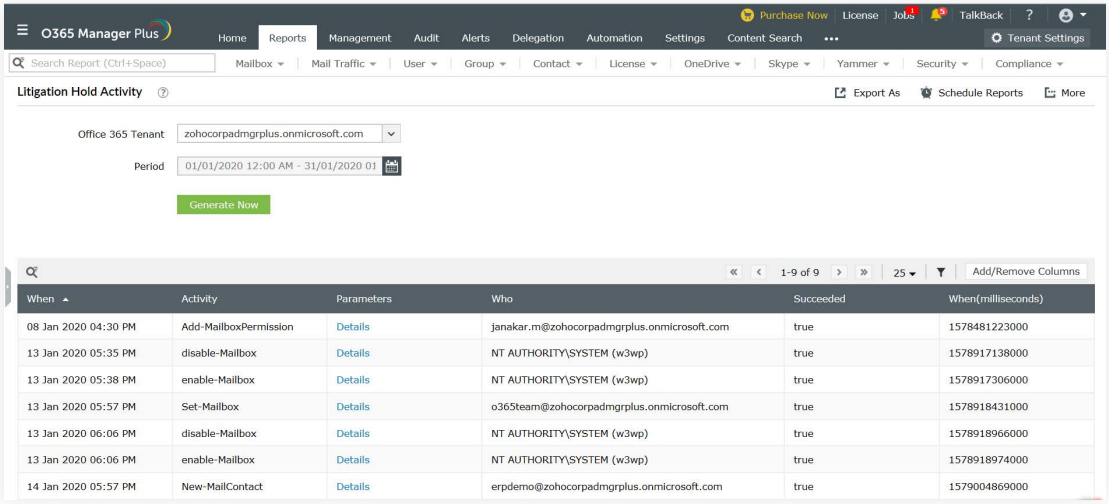


Figure 10. Litigation Hold Activity report.

5.1.1(c)(ii) InPlace Hold and eDiscovery Activity

M365 Manager Plus helps you identify all changes made to InPlace Hold objects, including information on the change, the administrator responsible for the change, and which parameters were changed. This report also provides details on all InPlace eDiscovery searches meant to search for content from your Exchange mailboxes.

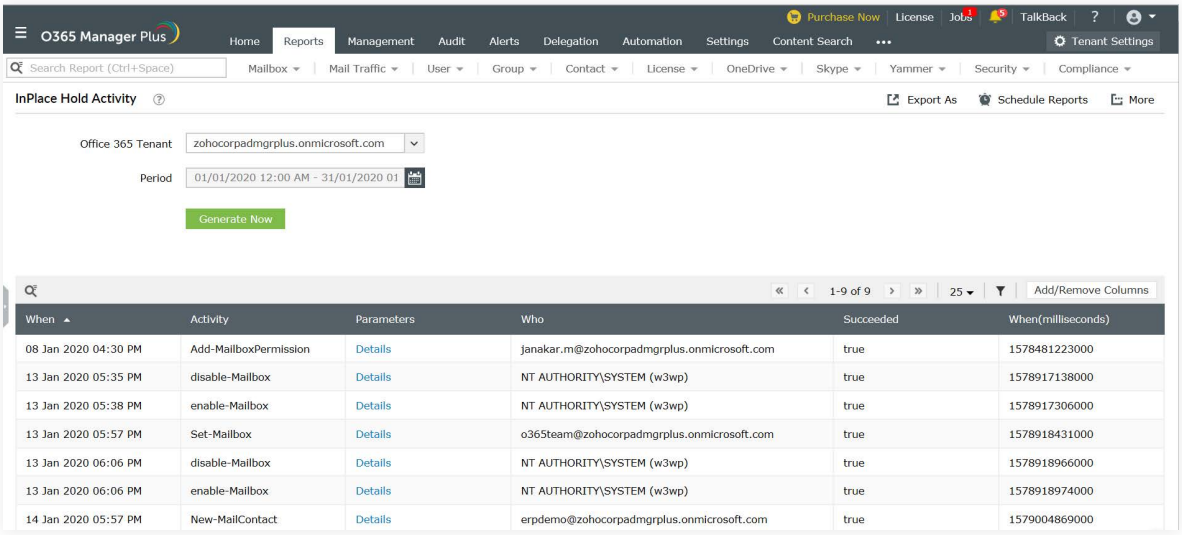


Figure 11. InPlace Hold and eDiscovery Activity report.

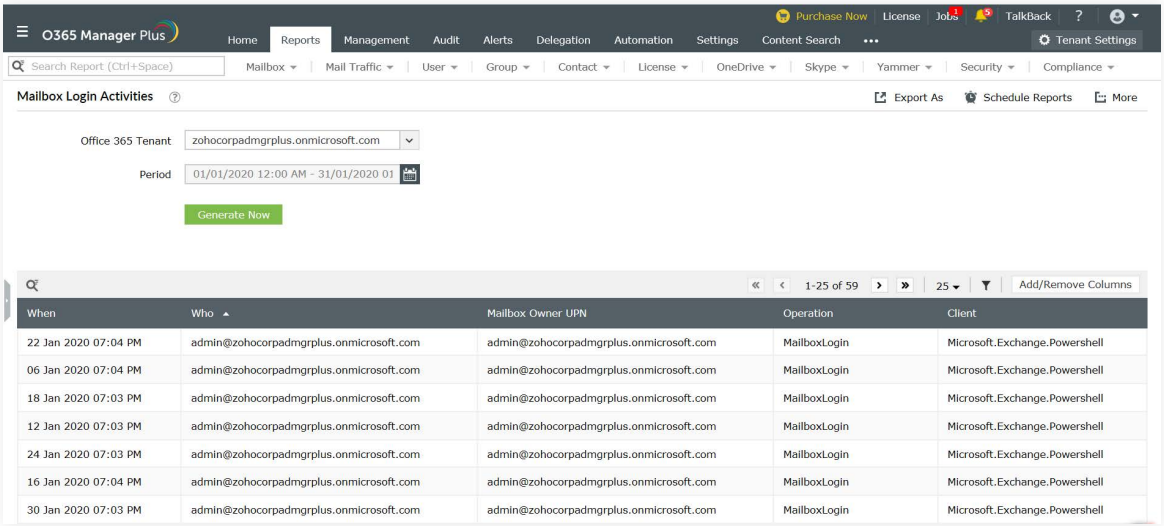


Figure 12. Mailbox Login Activities report.

5.1.2 User Activities

M365 Manager Plus provides reports on Exchange user activities, such as mailbox logins, along with details on who performed the activity, what activity was performed, status of the activity, client IP address, and more.

You can also monitor the activities performed by mailbox delegates and mailbox non-owners, as well as send as activities; mail, move, and delete activities; and more.

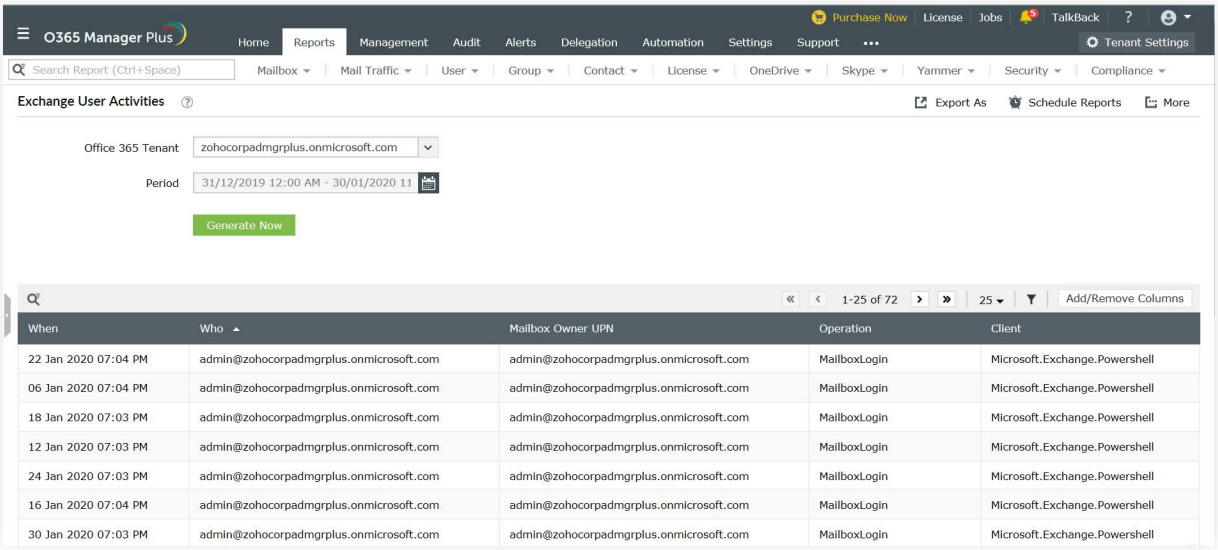


Figure 13. Exchange User Activities report.

5.2 User and mailbox security reports

M365 Manager Plus provides an array of user and mailbox security reports to enhance the security of your Microsoft 365 setup. With these reports you can:

- See which users were added and removed from admin roles to prevent unintended users from gaining privileged roles.
- View details on users who have access to shared mailboxes, as well as the type of access rights they have. This helps ensure correct permissions are granted only to desired users.
- Find passwords that are set to never expire in your Microsoft 365 setup so you can take corrective action.
- And more.

Figure 14. Mailbox and user security reports.

6. Get critical alerts for OneDrive for Business, Sway, Yammer, and Microsoft Teams

6.1 OneDrive for Business

With M365 Manager Plus, you can set customized alerts for OneDrive file and folder, sync, and sharing activities, along with the severity of the action performed, as shown in Figure 15.

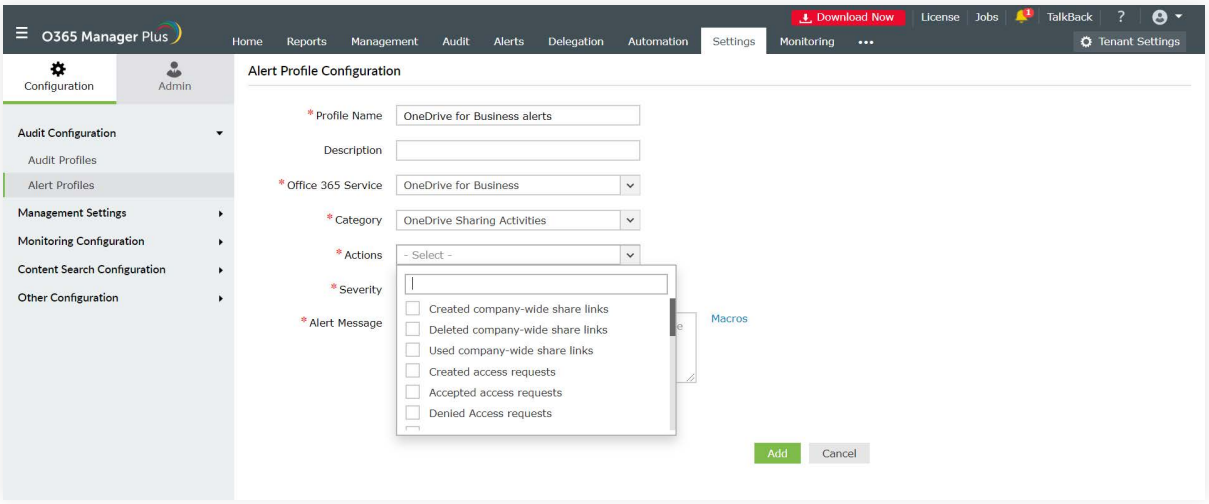


Figure 15. OneDrive for Business file sharing alerts.

6.2 Sway

M365 Manager Plus lets you audit and set alerts for various activities such as Sway creation, modification, duplication, deletion, and external sharing.

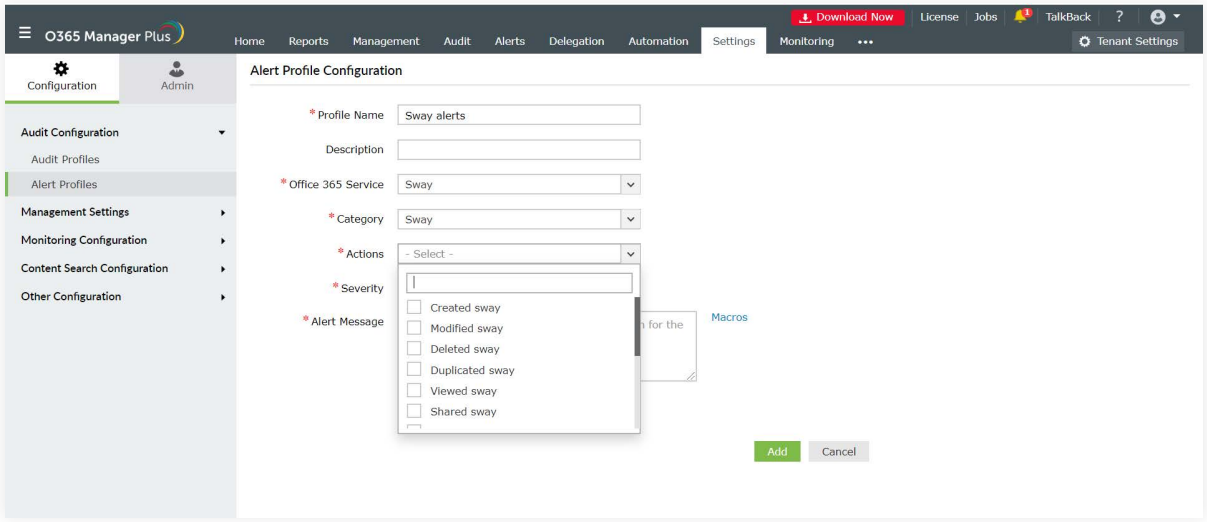


Figure 16. Set alerts for various actions performed in Sway.

6.3 Yammer

M365 Manager Plus helps get details about various admin activities, such as modifications to security configurations, delete settings, and private content mode. You can also view details on user activities including file sharing and message deletion.

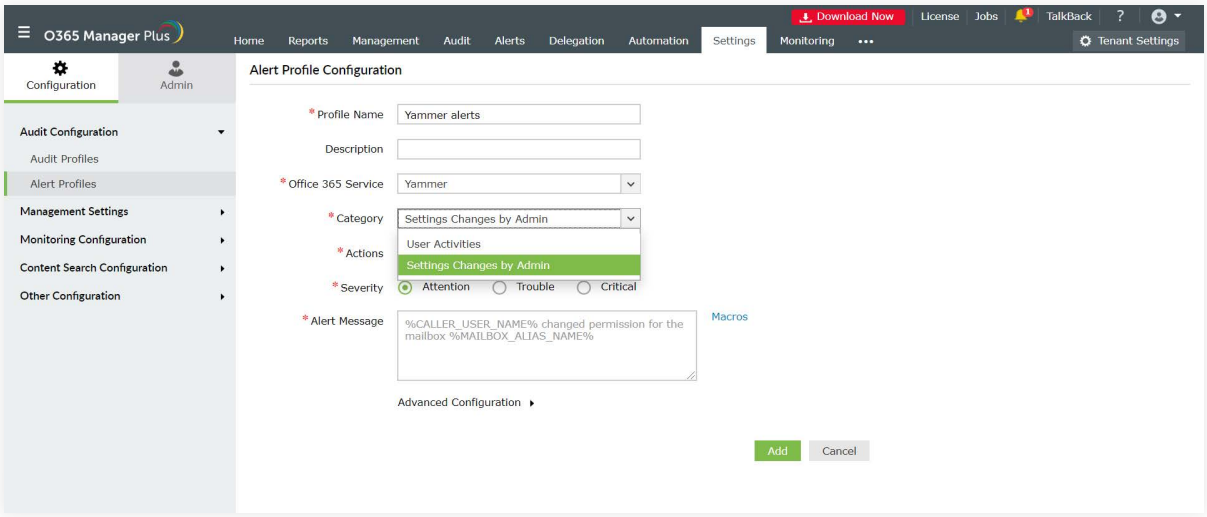


Figure 17. Set alerts for various user and admin actions in Yammer.

6.4 Microsoft Teams

M365 Manager Plus helps you audit events and setting changes in Microsoft Teams and raises alerts for these actions, as shown in Figure 18.

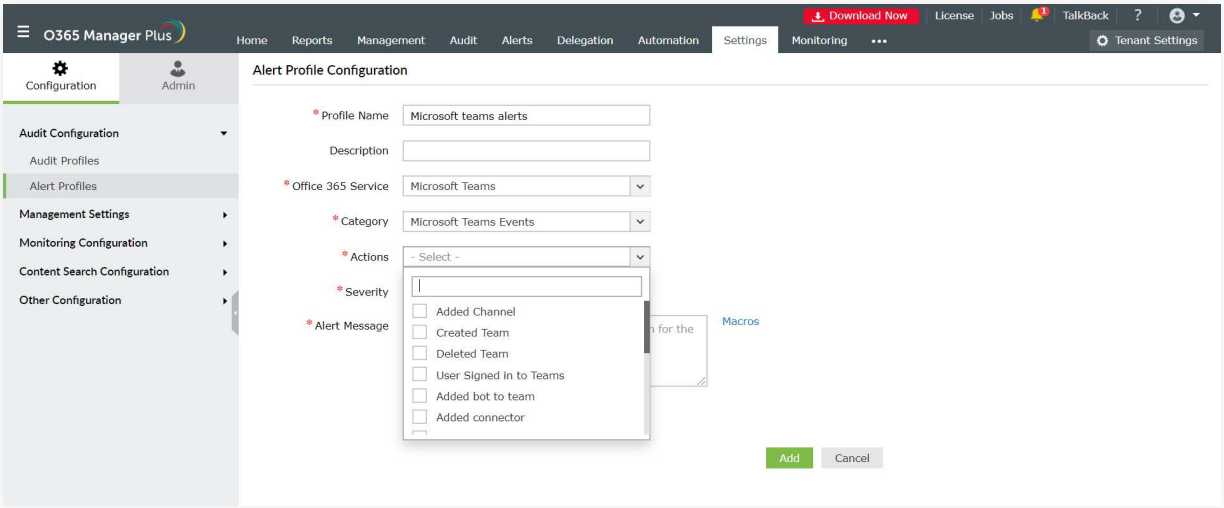


Figure 18. Set alerts for various actions performed in Microsoft Teams.

7. Summary

With M365 Manager Plus' comprehensive Microsoft 365 compliance and security module, you can:

- Generate reports for IT compliance regulations.
- Monitor email traffic to detect spam and malware.
- Run reports on Exchange and Azure admin activities, litigation holds, and more.
- Detect loss of sensitive data for faster disaster recovery.
- Get critical alerts on OneDrive for Business, Microsoft Teams, Yammer, Sway, and more.