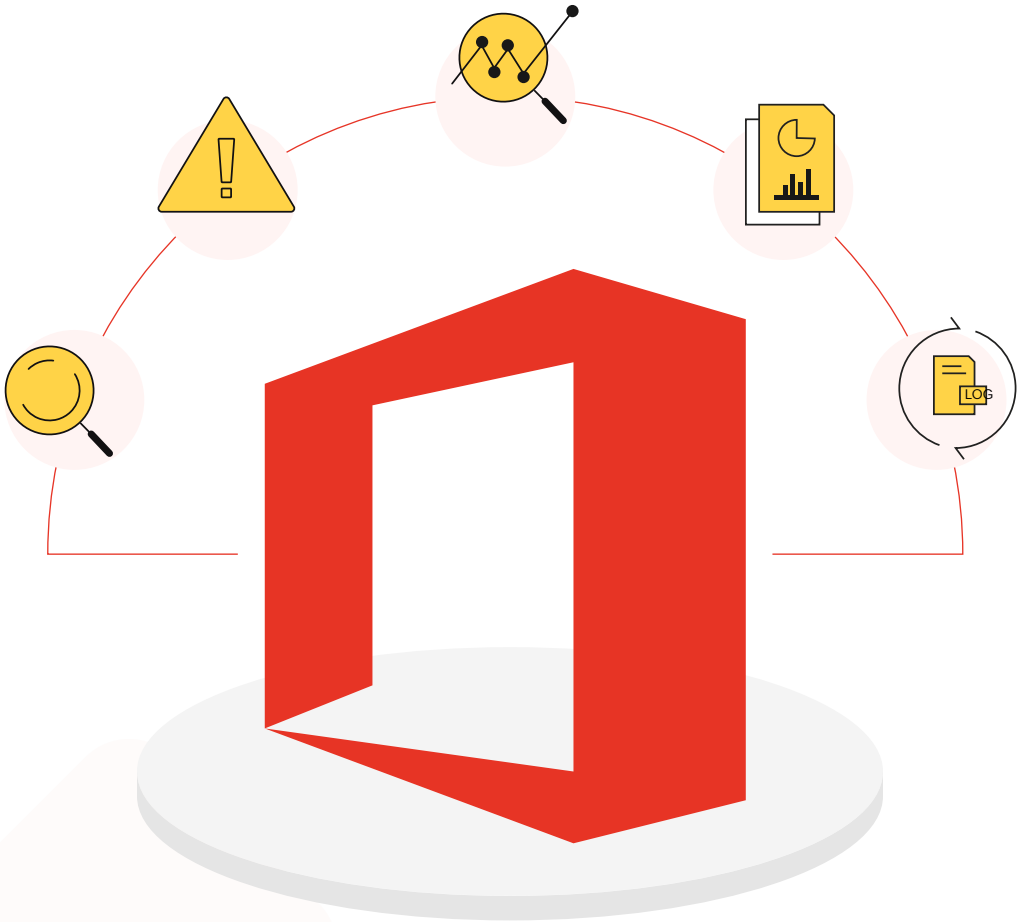
Microsoft 365 compliance:

5 PAIN POINTS AND HOW TO OVERCOME THEM



ManageEngine
M365 Manager Plus

Introduction

Microsoft Microsoft 365 is gaining rapid adoption among enterprises, with more than 200 million active commercial users every month. According to Gartner, 60 percent of global businesses will adopt cloud-based Microsoft suites by 2022.

This rapid migration to the cloud also brings with it some inevitable security responsibilities—one of the most crucial being meeting the requirements of IT compliance regulations such as PCI DSS, HIPAA, GLBA, and FISMA.

Non-compliance with such regulations can lead to hefty fines. For instance, non-compliance with HIPAA can result in fines of up to $250,000 and 10 years of imprisonment. However, the cost of non-compliance does not stop with penalties; it also includes the cost incurred due to business disruption, revenue loss, and decreased productivity, not to mention the intangible cost of a damaged reputation.

Regardless of the sector your organization belongs to, keeping up with the range of regulations that apply to you, and ensuring compliance with them, is an uphill task. As more and more corporate data migrates to a cloud-based productivity and collaboration suite like Microsoft 365, it becomes increasingly challenging to ensure compliance. On top of this, new regulations may emerge in the same time frame and make the situation worse.

Although Microsoft 365 is equipped with native capabilities to help you comply with various regulatory mandates, these features have a few limitations. For instance, the Microsoft 365 Security & Compliance Center, a one-stop portal intended to cater to your security and compliance needs, helps in numerous compliance activities such as archiving mailboxes, preventing data loss, managing devices, and assigning permissions. However, it quickly becomes quite overwhelming to configure these settings in the portal due to its nonintuitive user interface.

In this e-book, we will discuss five areas where Microsoft 365's native capabilities fall short in facilitating hassle-free compliance. And how with M365 Manager Plus, our holistic Microsoft 365 administration solution, you can overcome these shortcomings and ensure smooth compliance.

1. Microsoft 365 auditing

Microsoft 365 auditing is crucial to make your organization's compliance program foolproof, as it captures activities that occur across Microsoft 365 applications.

However, if you just use Microsoft 365's out-of-the-box features, you may be missing some crucial details that you need to thoroughly monitor user activity.

What differentiates a robust compliance program from a sloppy one is how granular of insights can be drawn from the organization's Microsoft 365 setup, and how effortlessly these insights can be used to meet compliance requirements. With M365 Manager Plus, you can seamlessly draw granular insights by generating and maintaining the audit details you need to meet compliance requirements.

With M365 Manager Plus, you can perform:

- Real-time auditing: Instead of fetching audit logs from the log repository each time, M365 Manager Plus keeps audit reports updated in real time.
- Profile-based auditing: Instead of going through the entire list of audit reports to find the right one, you can create your own profiles so you only see the required audit details.
- Advanced filtering: While Microsoft 365 only has provisions to filter audit logs based on certain attribute values, M365 Manager Plus facilitates filtering audit logs based on any attribute and performing multi-valued searches as needed.
- Data export: Microsoft 365 exports data only in CSV format. With M365 Manager Plus, you can export audit data in multiple formats, such as PDF, XLS, HTML, or CSV.

The M365 Manager Plus advantage:

- → Comprehensive location-based audit reports
- → Customizable audit reports
- → Provision to keep tabs on user activities performed outside business hours
- → Instant updates on important changes with customized alerts
- → User-based and group-based auditing
- → Audit log storage—indefinitely or for a period of your choice

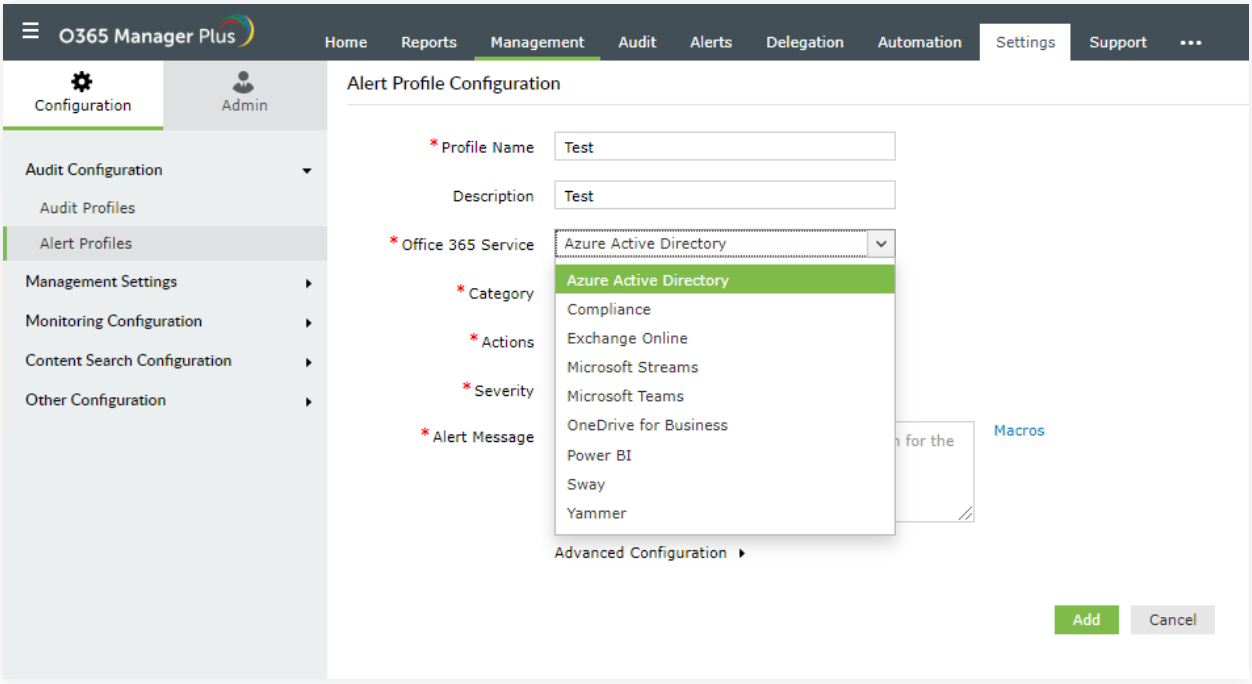
2. Microsoft 365 alerting

The more quickly suspicious activity is red-flagged, the better an organization's response can be to mitigate potential compliance roadblocks caused by such suspicious activities.

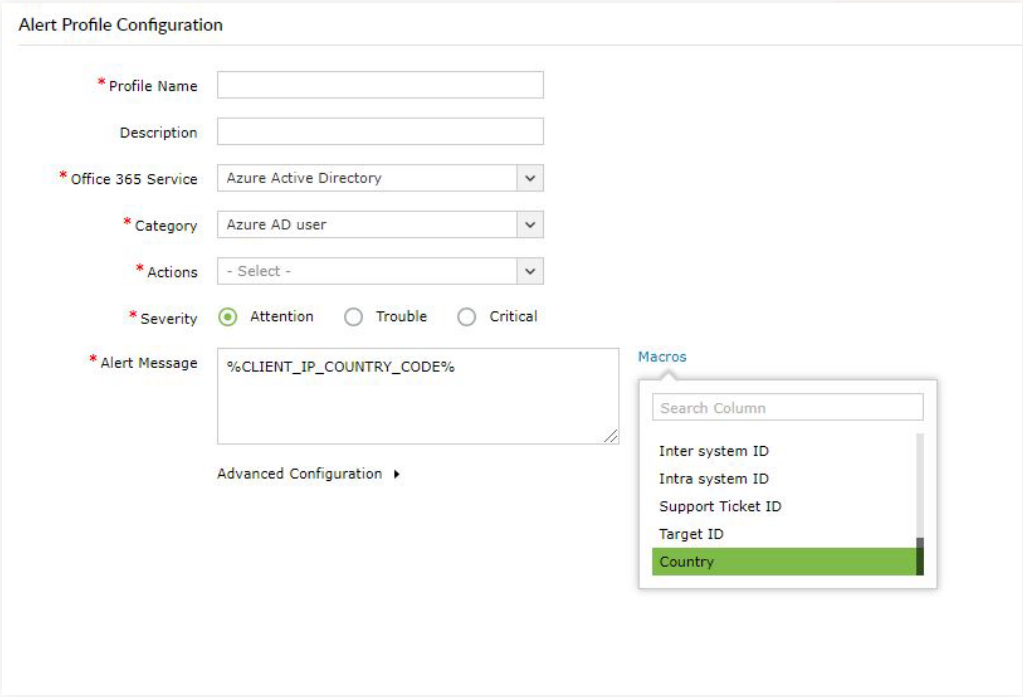
By configuring alert policies accordingly, you can comfortably avert the risk of noncompliance. Although Microsoft 365 has native provisions to set such alert policies, M365 Manager Plus goes several steps further and provides the level of customization that the current regulatory landscape warrants.

With M365 Manager Plus, you can:

Set alerts for Azure Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, and other Microsoft 365 services from a single place.



IP-based geolocation: See where users were when they performed a specific action based on the IP address of their devices. For example, admins can find the location (country) from where users log in to their Microsoft 365 accounts, and set alerts if a login occurs from a suspicious location.



3. Microsoft 365 monitoring

The real challenge of any compliance program is how proactive it is in maintaining compliance. Being able to keep your Microsoft 365 setup under continuous surveillance is crucial to identify any discrepancies that could pave the way for potential compliance roadblocks.

Though Microsoft 365 has the capability to monitor your Microsoft 365 setup fairly well, it comes with some limitations. For example, using Microsoft 365's native tools, you do not have provisions to granularly monitor Microsoft 365 services such as Exchange Online, Azure Active Directory, OneDrive for Business, and Skype for Business.

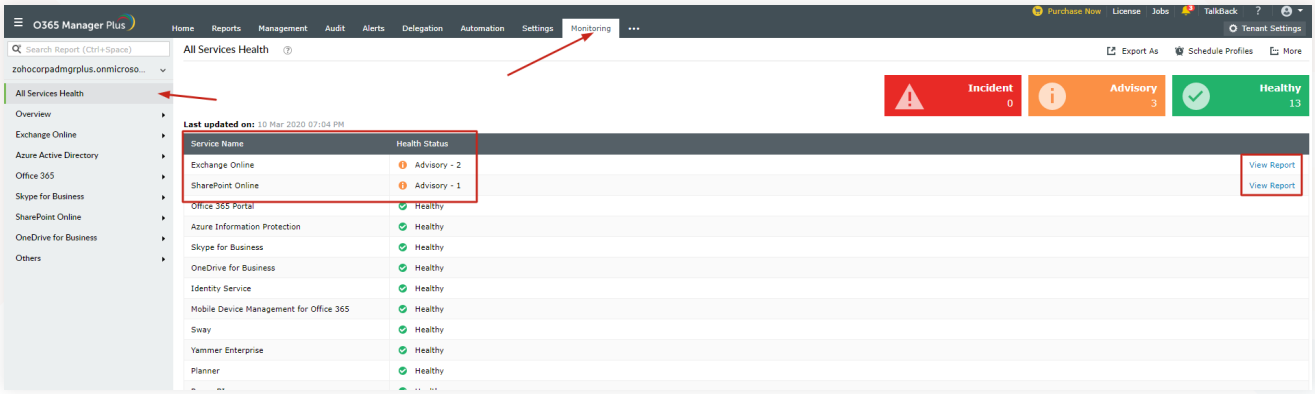
On the other hand, M365 Manager Plus offers:

Granular monitoring:

Each service in Microsoft 365 has its own set of features and endpoints. The service health dashboard of M365 Manager Plus has provisions to granularly monitor Microsoft 365 services as it provides granular details such as the number of incidents in features and endpoints of a service, severity of incidents, number of affected users, current status of the incident, start and end time of the incident, user Impact, and more.

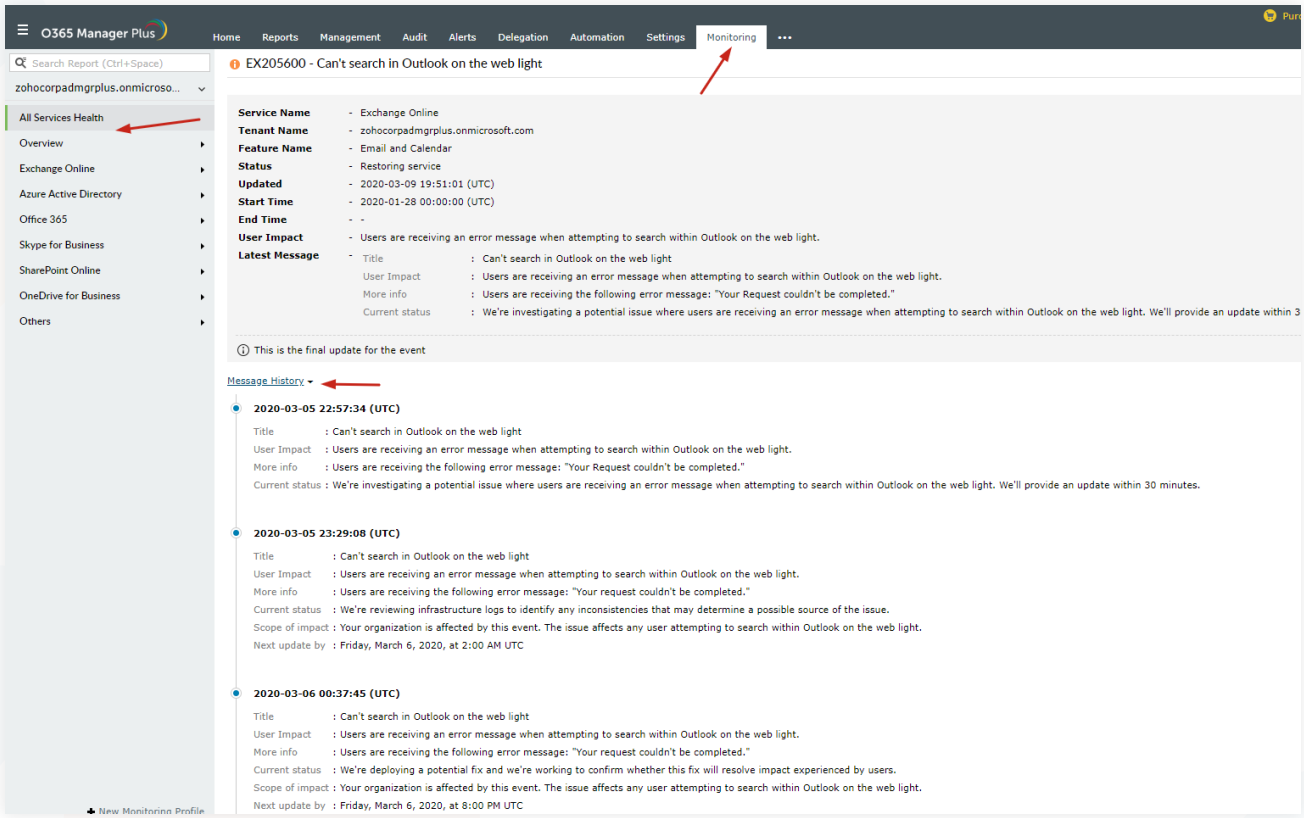
A central console:

With M365 Manager Plus, you can monitor the health of Exchange Online, Azure Active Directory, OneDrive for Business, Skype for Business, and ten other Microsoft 365 services, all from one central location.



Historical data:

With M365 Manager Plus, you gain access to historical Microsoft 365 service health monitoring data that is over 30 days old.



The M365 Manager Plus advantage:

- A single dashboard displaying the number of incidents and advisories occurring in various Microsoft 365 services including Exchange Online, Azure Active Directory, Microsoft Teams, and OneDrive for Business
- Graphical representation of service health
- Endpoint monitoring
- Provision to store all monitoring data for an indefinite period of time
- Dashboard displaying critical notifications and other alerts helps you stay updated about the status of Microsoft 365 services 24x7

4. Microsoft 365 reporting

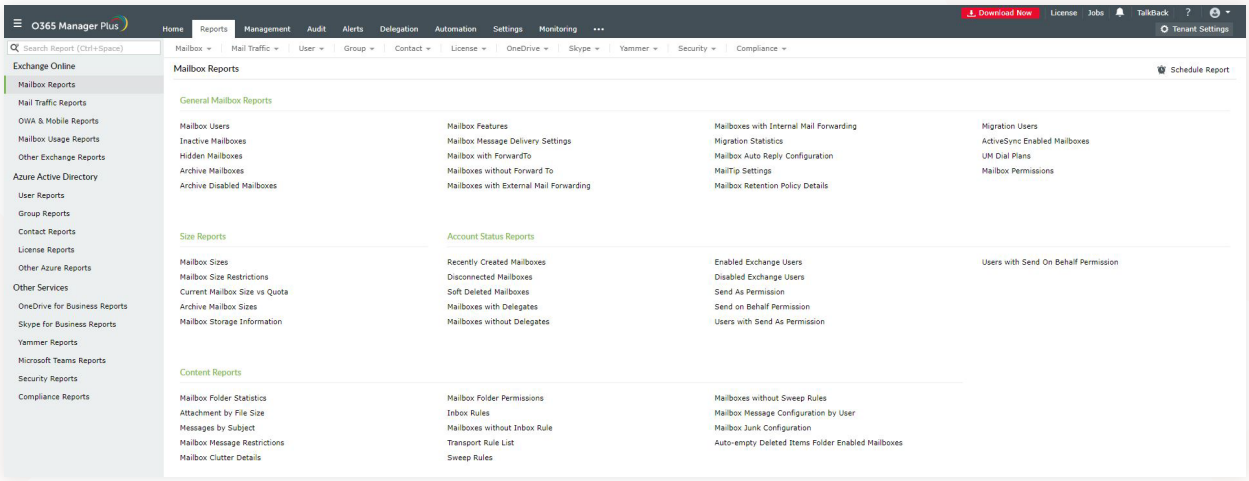
For any organization to stay compliant with the requirements of IT compliance mandates, it should have provisions to keep tabs on all administrative and user activities in its Microsoft 365 environment. Although this can be accomplished in Microsoft 365, the native tools' limitations could affect your organization's overall compliance posture.

For instance, although Microsoft 365 comes with its own set of preconfigured reports to gather extensive insights on what is really happening at the back end of your Microsoft 365 setup, Microsoft 365 can't present the insights in such a way that an auditor could readily understand. This is because the Reports dashboard in Microsoft 365 is fairly overwhelming due to its nonintuitive navigation and cluttered layout.

M365 Manager Plus helps tackle these limitations, allowing you to build a foolproof, proactive compliance program. With M365 Manager Plus, you get:

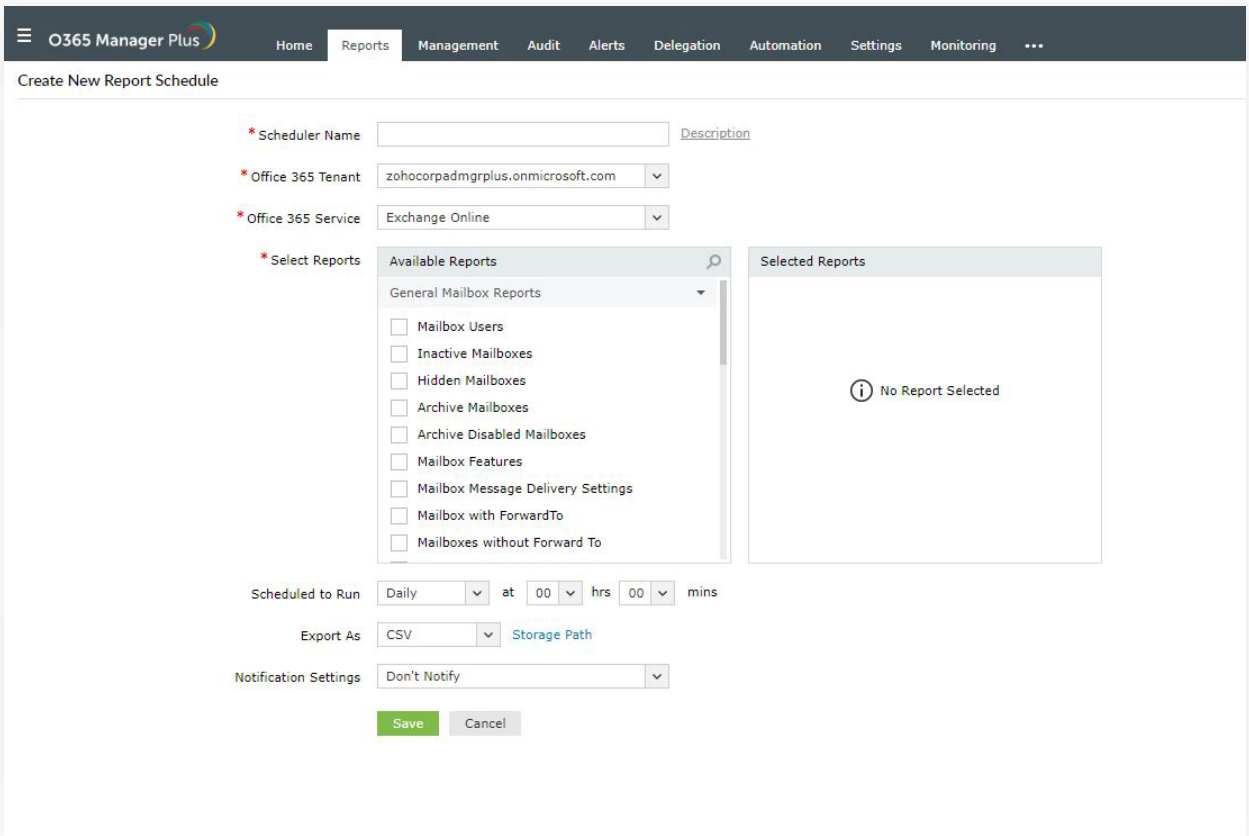
Compliance management

M365 Manager Plus' Compliance Reports tab lists industry-specific compliance mandates and the respective reports required to meet them. The compliance regulations covered by M365 Manager Plus include HIPAA, PCI DSS, SOX, GLBA, and FISMA.



Customizable scheduled reports

Microsoft 365 has provisions to schedule reports only on a weekly or monthly basis. On the other hand, with M365 Manager Plus, you can schedule the required report and have it sent to the administrator via email on a monthly, weekly, daily, or even hourly basis. Reports can be exported in PDF, CSV, XLS, or HTML format.



The M365 Manager Plus advantage:

- Comprehensive, granular reports to keep you updated about all Microsoft 365 services
  Summarized email traffic reports
- Dedicated reports on security and compliance
- Graphical representation of reports wherever applicable
- Attribute-level filtering
- Automatic report generation and emailing of reports (when scheduled)
- Unique reports for spam and malware recipients

5. Microsoft 365 audit log retention

From a compliance standpoint, audit logs are one of the most important tools in any Microsoft 365 setup, as they act as documented evidence of all the activities that happen in the Microsoft 365 environment. Being able to retain these audit logs is crucial. Microsoft 365 allows admins to search for audit logs with the help of the Security & Compliance Center. With an Microsoft 365 E3 license, you can retain the audit logs for 90 days. With an Microsoft 365 E5 license, you can retain them for a maximum of one year, after which they are deleted.

However, many major compliance regulations (except PCI DSS) mandate organizations retain audit logs for more than a year. The following table lists the event log retention requirements as mandated by major compliance regulations.

Regulation	Retention requirement
SOX	7 years
HIPPA	7 years
PCI-DSS	1 year
GLBA	6 years
FISMA	3 years

One way to overcome this limitation is to download and save audit logs manually. However, Microsoft 365's native export capability is limited to 1,000 entries. If all logs are exported, the limit is 50,000 items. This is still a huge drawback for many mid-sized and large organizations, as they likely hit the 50,000 item limit every day. This means an administrator would need to specify and generate at least one export every day. This is highly laborious and also risky since failing to do so will result in permanent loss of a day's worth of audit logs.

Alternatively, M365 Manager Plus enables you to retain your audit logs for an indefinite period of time in a separate storage platform, and restore them when required in a single click. With M365 Manager Plus, there is no restriction on the number of entries that can be exported. If need be, you can export the audit data as password-protected reports or archive them as password-protected files so they're tamper-proof, ensuring the integrity of the audit report. You can also specify when audit data should be archived and view summaries of scheduled archiving.