ManageEngine
M365 Manager Plus

An admin's guide to boosting your Microsoft 365 **Secure Score**

Introduction

Your Secure Score in Microsoft 365 is an indicator of how secure your Microsoft 365 environment currently is. The Secure Score is assigned based on the security configurations and activity enabled in your Microsoft 365 environment. When you log in to the Secure Score dashboard, it displays your current score compared to the maximum score that you can attain.

Though a perfect Secure Score doesn't provide an absolute guarantee that your organization won't be breached, it does ensure that you've taken additional steps towards mitigating the risk of security breaches. In this guide, we'll discuss five steps that you can implement in your Microsoft 365 setup to enhance your Secure Score.

However, Microsoft 365's native tools have a number of shortcomings, which means implementing these five steps can often pose a challenge. In this guide, we'll take a closer look at these challenges and how M365 Manager Plus not only makes it easy to implement these five steps, but also provides capabilities beyond what the native tool offers.

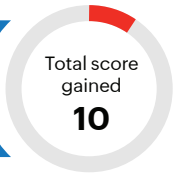
Boosting your Microsoft 365 Secure Score

Your organization can enhance its Microsoft 365 Secure Score by implementing the following steps:

1. Enable mailbox auditing for all users

If auditing is enabled in Microsoft 365, then by default it will only record folder permission updates by mailbox owners. To record all actions performed by mailbox owners, admins, or delegates, you need to enable mailbox auditing. By enabling mailbox auditing, you'll be able to search the audit logs and find non-owner mailbox accesses, breaches of privilege by delegated users or admins, and other potentially harmful actions. Such comprehensive auditing of mailbox activities can help organizations detect security breaches as well as stay compliant with IT regulatory standards.

By enabling mailbox auditing, your organization can boost its Secure Score by 10 points.



Enabling mailbox auditing in a few clicks using M365 Manager Plus

Enabling mailbox auditing is not supported by the Microsoft 365 Security & Compliance Center or the Exchange admin center. In order to enable this feature, administrators have to use PowerShell. But even if auditing is enabled using PowerShell scripts, not all actions are audited by default. This means admins often invest a great deal of time in writing long and complex PowerShell scripts.

This is where M365 Manager Plus' management feature comes in handy. In just a few clicks, administrators can easily enable auditing for any number of mailboxes.

Learn how to enable Exchange Online auditing using M365 Manager Plus.

Auditing using Microsoft 365 Security and Compliance Center provides limited visibility into audit logs which is insufficient for performing security audits and investigations.

The 90-day log storage limitation forces admins to export and save audit logs. Aside from increasing admins' workloads, this takes up a large amount of storage space in the organization's database.

M365 Manager Plus overcomes these limitations with the following features:

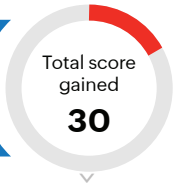
- **Indefinite log storage:** Audit logs are not only stored indefinitely, but are also easy to access during compliance audits and security investigations.
- **Audit log archival:** Place audit logs in an archive at the admin's convenience and restore deleted audit logs with a single click.

You can read more about M365 Manager Plus' auditing feature here, and also learn how to create your own audit views.

2. Disable mail forwarding by clients to external email addresses

One of the methods hackers are increasingly using to exfiltrate data is setting up client-side forwarding rules to forward emails to external email addresses. There could be hundreds of these forwarding rules, which makes it tough for admins to detect malicious events, even with rigorous auditing. Besides, if employees decide not to keep a copy of the forwarded emails in their mailboxes, these emails won't be archived and can't be used in the future.

By disabling the client's capability of forwarding emails to external email addresses, you can add 20 points to your organization's security score.



How M365 Manager Plus' capability to perform management actions from reports goes a step further than Microsoft 365's native tool

If admins were to disable email forwarding by modifying the Default Role Assignment Policy or by disabling forwarding set through Inbox Rules, they would still have to remove the auto-forwarding implemented earlier. This requires admins to do some PowerShell scripting.

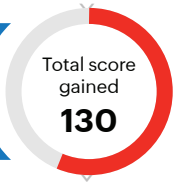
Using M365 Manager Plus' provision to perform management actions from reports, admins can not only generate reports, but also perform management actions from the reports themselves. For instance, admins can generate the Mailboxes with External Mail Forwarding report, then from this report disable external mail forwarding for all clients who have enabled this capability. It's also easy for admins to set exceptions to external mail forwarding with a few clicks.

Learn how to disable mail forwarding by clients to external email addresses using M365 Manager Plus.

3. Enable multi-factor authentication for Azure AD privileged roles and users

Multi-factor authentication (MFA) is a crucial component in ensuring secure access to an organization's network by protecting user identities and ensuring that users are actually who they claim to be. By implementing MFA for all user accounts, and especially for accounts with privileged roles, organizations can prevent adversaries from gaining access to critical devices and data, even if accounts have their credentials compromised.

By implementing MFA for all the users and Azure AD privileged roles in an Microsoft 365 environment, you can increase your Secure Score by 100 points.



Why Microsoft 365's native tool isn't good enough for bulk management

While Microsoft 365 provides the option to configure MFA, its UI is not very user-friendly. To enable MFA, you need to work between different tabs for selecting users and configuring settings. M365 Manager Plus, on the other hand, simplifies this task by allowing you to configure MFA for multiple users from a single console in just a few clicks.

What's more, Microsoft 365's native tool normally allows for only one tenant to be worked with at a time. For MSPs managing multiple clients, there's a need for unified access to multiple tenants. To work with multiple tenants, delegated admin permissions need to be created, which is a cumbersome task.

Securing multiple tenants from a single console: M365 Manager Plus lets you configure multiple tenants as well as configure MFA for users belonging to any of the tenants from the same console.

Learn how to configure MFA for your Microsoft 365 setup using M365 Manager Plus.

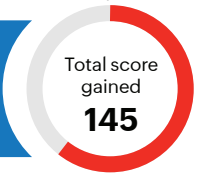
4. Review audit data, the Mailbox Access by Non-Owners report, and the Malware Detections report

It's necessary for administrators to comprehensively review audit logs to reduce the chances of a hacker operating undetected in your organization's Microsoft 365 environment for a long period.

Malware is one of the most popular attack vectors against Microsoft 365 setups. By reviewing the Malware Detections report, admins can get an idea of the amount of malware attacks their organization is subjected to, and can decide whether they need to harden their malware mitigation policy further.

Threats to your organization aren't just from outsiders, but insiders too. To thwart any malicious insider from accessing other users' emails, admins must thoroughly review the Mailbox Access by Non-Owners report.

By reviewing these reports, organizations can gain another 15 Secure Score points.



How M365 Manager Plus' report scheduling capability makes reviewing audit data easier than Microsoft 365's native tool

M365 Manager Plus enables audit and monitoring reports to be automatically scheduled and emailed to administrators. The tool also provides a provision to refine scheduled reports by selecting the desired attributes only, share schedules with other technicians, and more.

Using the native tool, admins can only download a maximum of 50,000 log entries to a CSV file from a single audit log search, which isn't a lot (especially for mid-sized and large organizations). This limited scope makes reviewing audit logs a tough task.

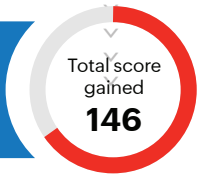
Unrestricted log export: M365 Manager Plus has no restriction on the number of logs that can be exported, which makes it easy to review the audit logs all at once. Admins can export or archive logs in PDF, XLS, and HTML formats as well.

Read more about M365 Manager Plus' comprehensive reporting capabilities, including reporting on mailbox access by non-owners.

5. Configure non-global administrative roles

Though it's a good practice to have more than one global administrator, having too many can have disastrous consequences if one of these accounts were to be breached. It's better to implement the policy of least privilege, and delegate responsibilities to admins with lesser roles.

By configuring non-global administrative roles, organizations can gain 1 Secure Score point.



Why you should delegate tasks using M365 Manager Plus instead of the Microsoft 365 admin center

The native Microsoft 365 portal has a set of admin roles with a predetermined scope of activity and doesn't allow custom admin roles to be created.

Granular non-administrative roles: Microsoft 365 Plus allows you to create custom non-administrative roles for technicians so you can delegate a specific set of activities to them. This lets admins create help desk roles with the least possible privilege, which reduces the risk of these accounts causing damage if they're ever compromised.

Read more about granular help desk delegation using M365 Manager Plus, as well as how to create custom help desk roles.

Top Three

M365 Manager Plus security features

1. Comprehensive Exchange Online auditing and reporting to secure your organization from hackers.

   Exchange Online reporting

2. Hassle-free Azure AD auditing and reporting to track users, groups, contacts, and licenses.

   Azure AD reporting

3. Exhaustive reporting on all administrator activities to strengthen your organization's security.

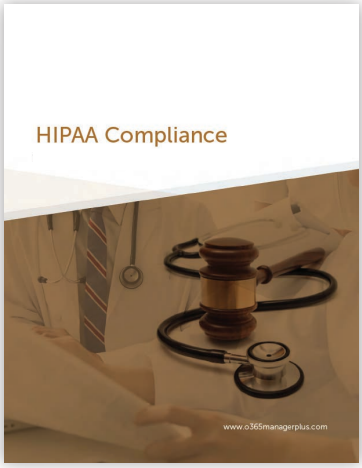
   Microsoft 365 activity reports

IT compliance checklists for **SOX, FISMA, GLBA, HIPAA,** and **PCI DSS**

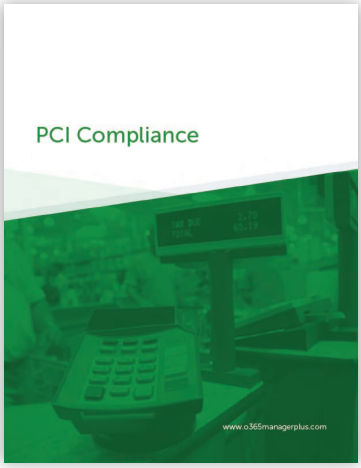
[Download SOX compliance checklist]

[Download FISMA compliance checklist]

[Download GLBA compliance checklist]



[Download HIPAA compliance checklist]



[Download PCI DSS compliance checklist]

ManageEngine
M365 Manager Plus

M365 Manager Plus is an extensive Microsoft 365 tool used for reporting, managing, monitoring, auditing, and creating alerts for critical incidents. With its user-friendly interface, you can easily manage Exchange Online, Azure AD, Skype for Business, OneDrive for Business, Microsoft Teams, and other Microsoft 365 services from a single console.

$ Get Quote Download