4 MUST-AUDIT MICROSOFT 365 ACTIVITIES

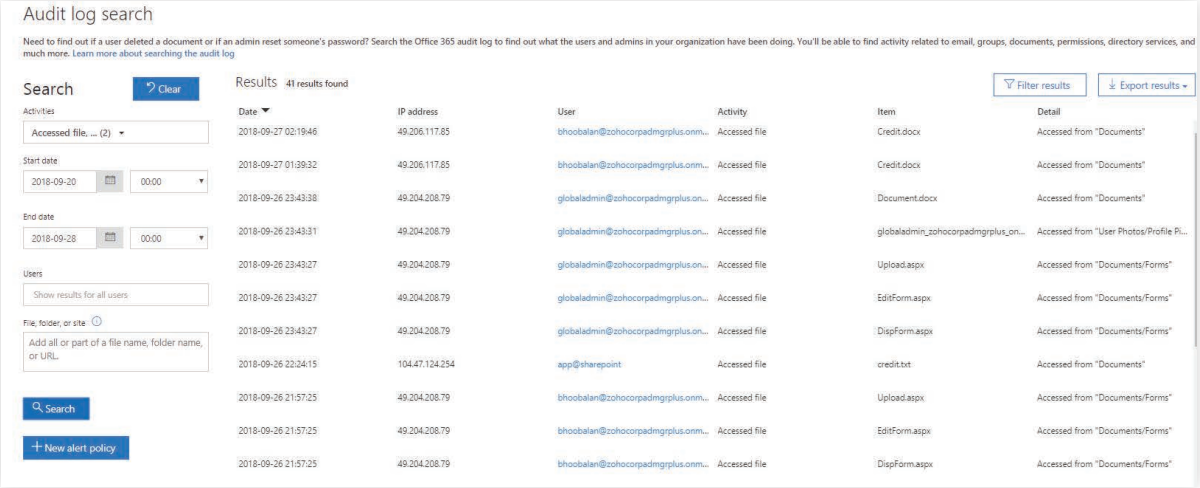
ManageEngine
M365 Manager Plus

Introduction

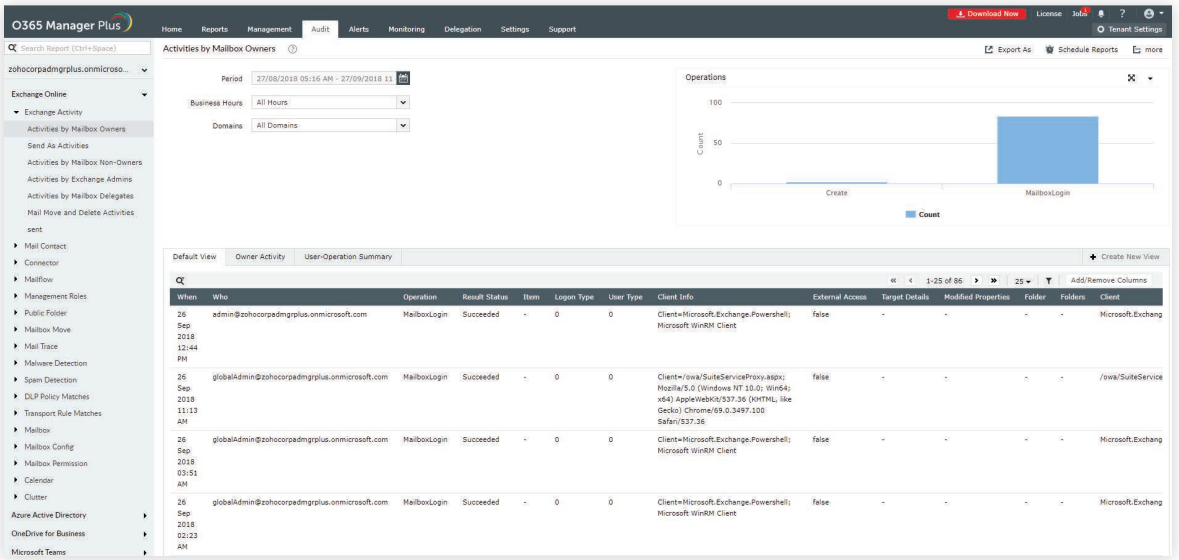
Auditing and security always go hand-in-hand, especially when it comes to workplace activities. In any large organization, a ton of audit logs are generated every second, making it difficult to track and interpret this information.

Auditing activity in M365 Manager Plus

When it comes to tracking activity, Microsoft 365 doesn't offer much help, as it doesn't provide any comprehensive audit reports. Instead, users have to retrieve any required audit logs using the Audit log search option. Additionally, Microsoft 365 only has a 90-day audit window; any audit logs older than 90 days are automatically purged from Microsoft 365.



On the other hand, M365 Manager Plus has more than 700 preconfigured reports that can be viewed in a single click. M365 Manager Plus places no restricting on audit data, allowing audit logs to be stored and accessed indefinitely. All reports can be automatically delivered to your inbox at regular intervals in PDF, XLS ,HTML, or CSV formats.



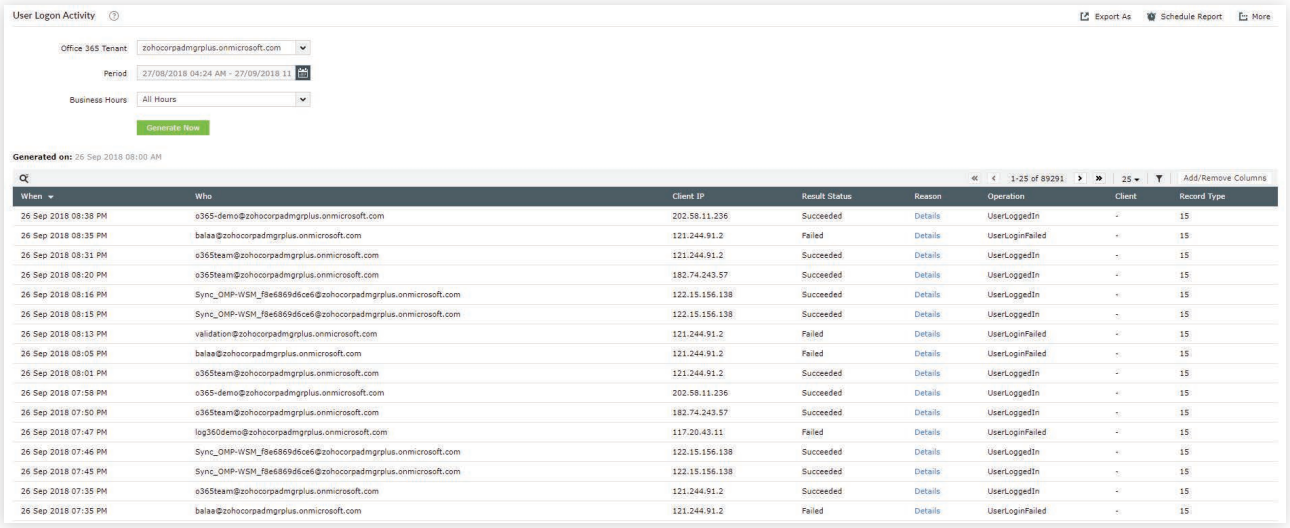
Activities that must be audited

Microsoft 365 auditing is an effective way to gain insight into user activities and insider threats. Although there's a plethora of activities that should be audited, there are four activities you must audit if you want to identify common threats like brute-force attacks, insider attacks, and elevation of privilege attacks. The four activities that must be audited are:

- User accesses
- Admin activities
- File accesses and sharing
- Changes to Microsoft 365 policies

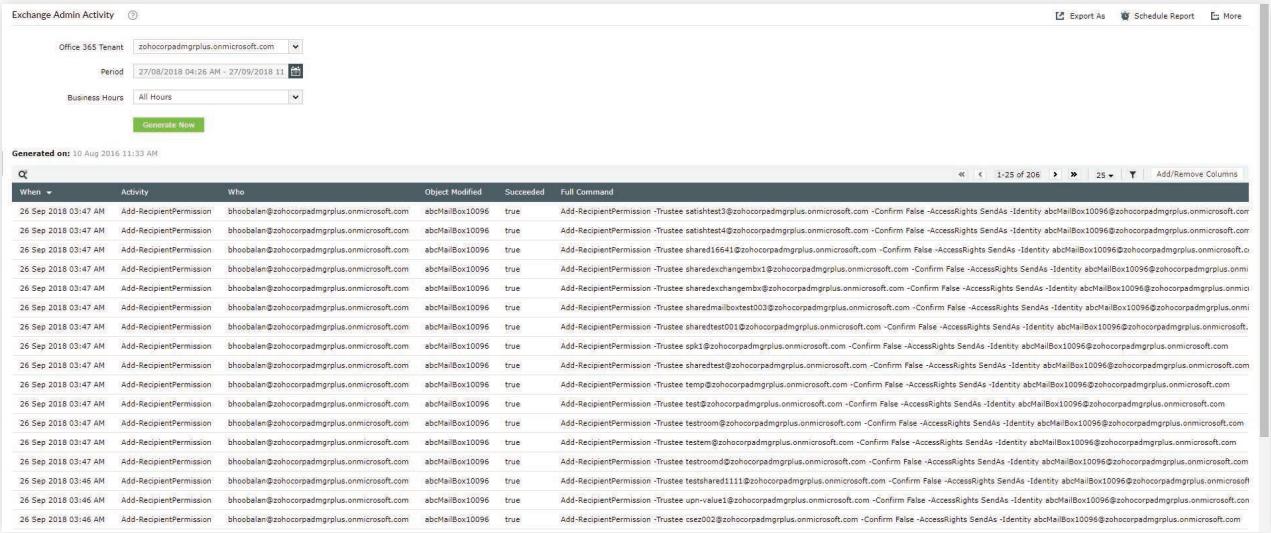
User accesses

You should know who is accessing your Microsoft 365 subscription, when, and from where. Establishing a baseline of normal user access behavior allows you to spot anomalous or suspicious user activities. A user trying to sign in from a country where your organization doesn't have any presence is clearly suspicious, so you should track the time and location of logins. Additionally, spikes in repeated login attempts can alert you to a potential brute-force attack.



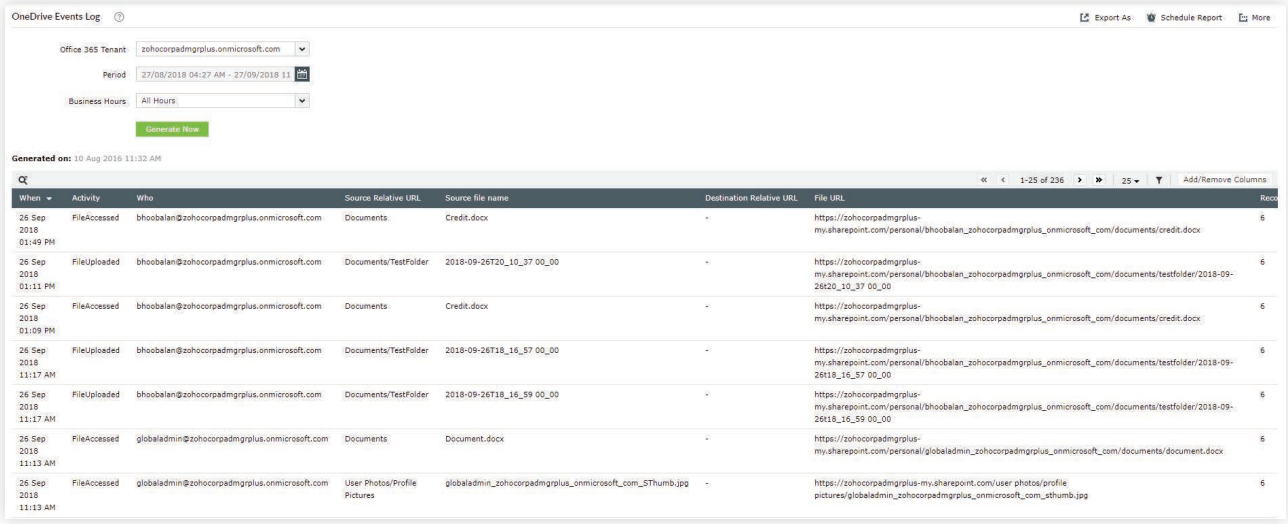
Admin activities

Once attackers gain access to your environment, they'll often try to elevate their privileges to gain more control and access to your sensitive data. The same can be said about malicious insiders. Monitoring changes to admin roles and access rights can alert you to potential internal and external threats.



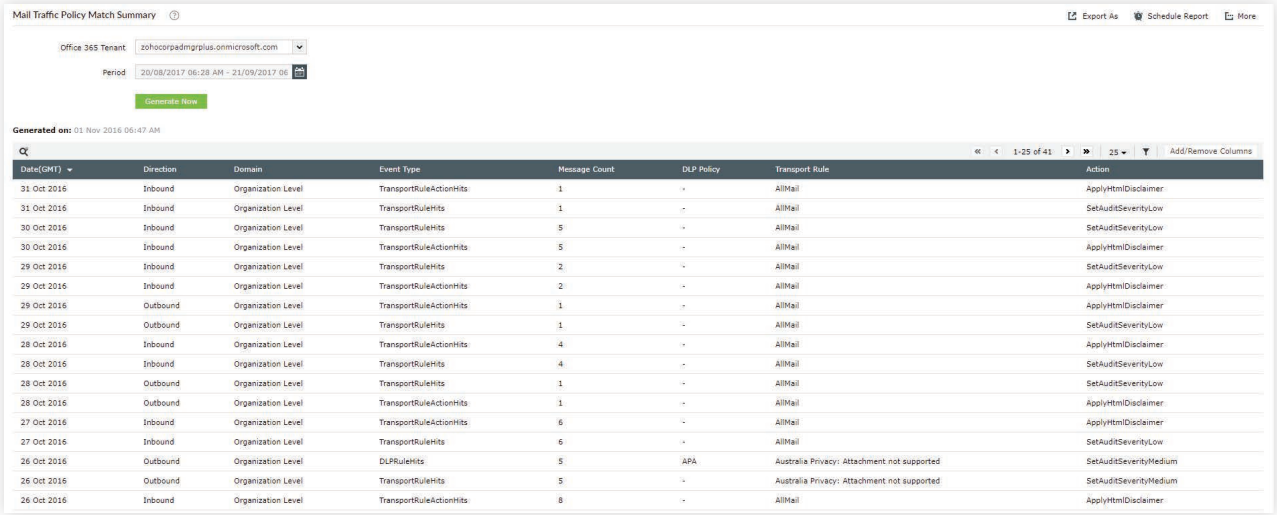
File accesses and sharing

Monitoring changes to file share permissions and policies in OneDrive for Business can alert you to the early signs of a potential data breach. Additionally, monitoring file activities of user—including file uploads, deletions, edits, and restorations—can help you to detect and investigate anomalous activities.



Changes to Microsoft 365 policies

This includes changes to Exchange malware and content filtering policies, which may enable spammers to send phishing emails and malicious attachments. These changes could also weaken your organization's password policies.



Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine
M365 Manager Plus

M365 Manager Plus is an extensive Microsoft365 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 Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, and other Microsoft 365 services from a single console.

$ Get Quote Download