ManageEngine
M365 Manager Plus

Microsoft 365 Audit Logs Archiving

Why do you need an Archival Solution?

www.microsoft365managerplus.com

Introduction

We live in a world where the threat of compromise is ever-present, ever-changing, and ever-growing. Never before has there been so much focus on the need for security—enough to make it an integral part of choosing new solutions, platforms, and applications. And for cloud platforms like Microsoft 365, there's an even greater emphasis on the importance of security.

Audit logs are critical for understanding the nature of security incidents, both during an active investigation and after when analyzing the incident.

Microsoft 365 audit data archival and restoration.

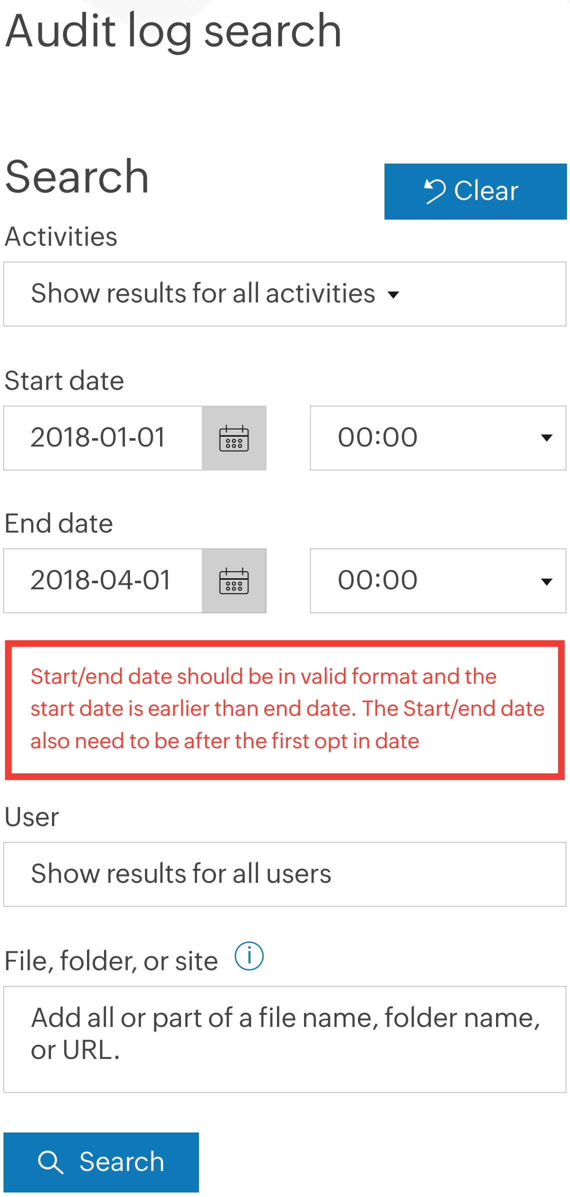
If your organization is serious about auditing all user and admin activity in Microsoft 365, then you'll have to deal with the volumes of audit logs that are added to your database every minute. These audit logs contain traces of all types of activity, ranging from simple file renames to password resets and unwanted login attempts.

Why do you need an archival solution?

Auditing every activity happening in your Microsoft 365 environment requires you to analyze all the logs generated by various services and user activities. And to comply with regulatory mandates, this audit log data must be archived—but Microsoft 365 doesn't make archiving easy.

The 90-day window.

Limitation: Microsoft 365 offers a unified audit logging service across key workloads, which is accessed through the Security and Compliance Center. However, audit entries in the Security and Compliance Center are retained for only 90 days, after which they're purged. Organizations that need long-term access to audit report items—such as the seven years worth of data required by some compliance regulations—should be aware of this limitation.



Audit log search

Search

Activities

Show results for all activities

Start date

2018-01-01 00:00

End date

2018-04-01 00:00

Start/end date should be in valid format and the start date is earlier than end date. The Start/end date also need to be after the first opt in date

User

Show results for all users

File, folder, or site

Add all or part of a file name, folder name, or URL.

Solution: You can manually download and save audit logs every 90 days, but failing to do so would result in the permanent loss of logs. On the other hand, M365 Manager Plus holds audit logs indefinitely. Therefore, you can choose to archive audit logs at your convenience, like when your database is running out of space. You can also restore deleted audit logs in M365 Manager Plus in a single click.

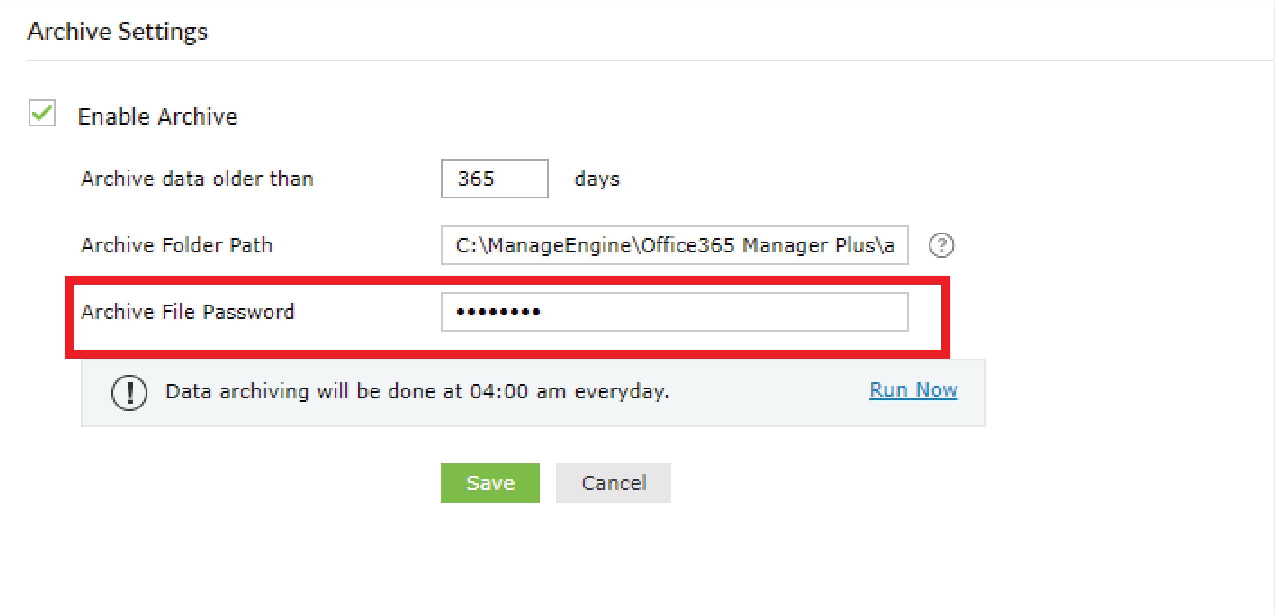
Exporting audit logs.

Limitation: When exporting specific audit logs from Microsoft 365, the export is limited to 1,000 entries—unless all logs are exported, in which case the limit is 50,000 items. This is severely limiting since some mid-sized and large organizations hit the 50,000 item limit every day. Manually exporting logs for organizations of this size requires an administrator to specify and generate at least one export every day, hoping that the time delay in capturing audit report entries doesn't result in an incomplete report.

Since these exports are delivered as simple CSV files, there's also no accountability involved in the accuracy of the data, meaning there's nothing stopping an administrator from making up data or removing evidence of their own wrongdoing.

Solution: M365 Manager Plus imposes no restriction on the number of entries that can be exported. You can export the audit data as password-protected reports or archive them as password-protected files so they're tamper-proof.

archive-settings



Archive Settings

☑ Enable Archive

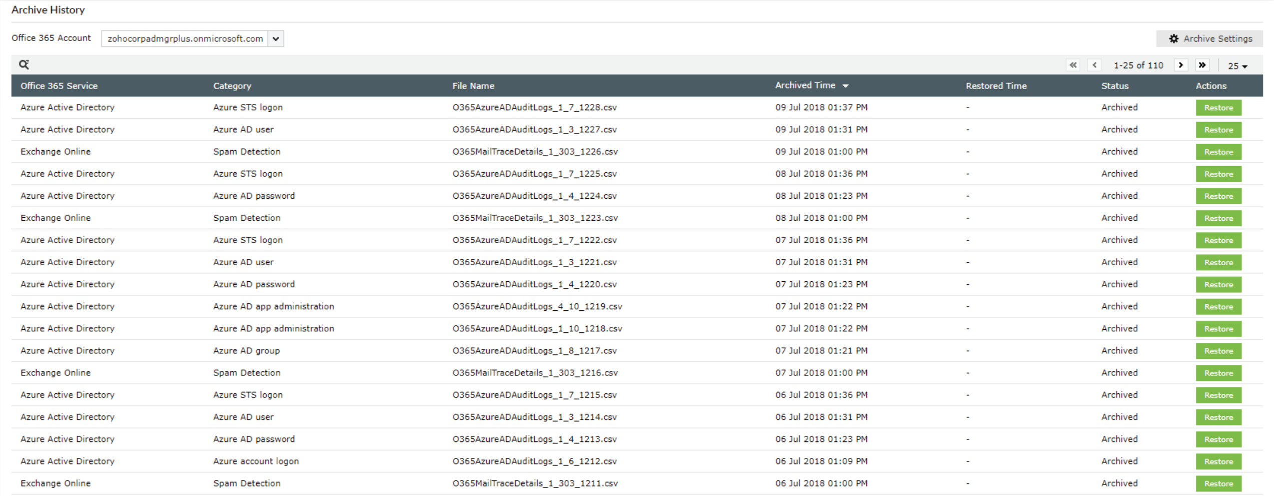
Archive data older than	365	days
Archive Folder Path	C:\ManageEngine\Office365 Manager Plus\a	
Archive File Password	••••••••	

Data archiving will be done at 04:00 am everyday.

Audit data archiving and restoration with M365 Manager Plus.

M365 Manager Plus allows you to archive Microsoft 365 audit logs in a separate storage platform, and restore them when required in a single click. You can also:

- Specify when audit data should be archived.
- Store archived audit logs as password-protected files.
- View summaries of scheduled archiving.



Archive History

Office 365 Account: zohocorpadmgrplus.onmicrosoft.com

Office 365 Service	Category	File Name	Archived Time	Restored Time	Status	Actions
Azure Active Directory	Azure STS logon	O365AzureADAuditLogs_1_7_1228.csv	09 Jul 2018 01:37 PM	-	Archived	Restore
Azure Active Directory	Azure AD user	O365AzureADAuditLogs_1_3_1227.csv	09 Jul 2018 01:31 PM	-	Archived	Restore
Exchange Online	Spam Detection	O365MailTraceDetails_1_303_1226.csv	09 Jul 2018 01:00 PM	-	Archived	Restore
Azure Active Directory	Azure STS logon	O365AzureADAuditLogs_1_7_1225.csv	08 Jul 2018 01:36 PM	-	Archived	Restore
Azure Active Directory	Azure AD password	O365AzureADAuditLogs_1_4_1224.csv	08 Jul 2018 01:23 PM	-	Archived	Restore
Exchange Online	Spam Detection	O365MailTraceDetails_1_303_1223.csv	08 Jul 2018 01:00 PM	-	Archived	Restore
Azure Active Directory	Azure STS logon	O365AzureADAuditLogs_1_7_1222.csv	07 Jul 2018 01:36 PM	-	Archived	Restore
Azure Active Directory	Azure AD user	O365AzureADAuditLogs_1_3_1221.csv	07 Jul 2018 01:31 PM	-	Archived	Restore
Azure Active Directory	Azure AD password	O365AzureADAuditLogs_1_4_1220.csv	07 Jul 2018 01:23 PM	-	Archived	Restore
Azure Active Directory	Azure AD app administration	O365AzureADAuditLogs_4_10_1219.csv	07 Jul 2018 01:22 PM	-	Archived	Restore
Azure Active Directory	Azure AD app administration	O365AzureADAuditLogs_1_10_1218.csv	07 Jul 2018 01:22 PM	-	Archived	Restore
Azure Active Directory	Azure AD group	O365AzureADAuditLogs_1_8_1217.csv	07 Jul 2018 01:21 PM	-	Archived	Restore
Exchange Online	Spam Detection	O365MailTraceDetails_1_303_1216.csv	07 Jul 2018 01:00 PM	-	Archived	Restore
Azure Active Directory	Azure STS logon	O365AzureADAuditLogs_1_7_1215.csv	06 Jul 2018 01:36 PM	-	Archived	Restore
Azure Active Directory	Azure AD user	O365AzureADAuditLogs_1_3_1214.csv	06 Jul 2018 01:31 PM	-	Archived	Restore
Azure Active Directory	Azure AD password	O365AzureADAuditLogs_1_4_1213.csv	06 Jul 2018 01:23 PM	-	Archived	Restore
Azure Active Directory	Azure account logon	O365AzureADAuditLogs_1_6_1212.csv	06 Jul 2018 01:09 PM	-	Archived	Restore
Exchange Online	Spam Detection	O365MailTraceDetails_1_303_1211.csv	06 Jul 2018 01:00 PM	-	Archived	Restore

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 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 Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, and other Microsoft 365 services from a single console.

$ Get Quote

Download