

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.

Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search Clear Filter results Export results

Results 41 results found

Activities	Date	IP address	User	Activity	Item	Detail
Accessed file, ... (2)	2018-09-27 02:19:46	49.206.117.85	bhoobalan@zohocorpdmgrplus.onm...	Accessed file	Credit.docx	Accessed from "Documents"
	2018-09-27 01:39:32	49.206.117.85	bhoobalan@zohocorpdmgrplus.onm...	Accessed file	Credit.docx	Accessed from "Documents"
	2018-09-26 23:43:38	49.204.208.79	globaladmin@zohocorpdmgrplus.onm...	Accessed file	Document.docx	Accessed from "Documents"
	2018-09-26 23:43:31	49.204.208.79	globaladmin@zohocorpdmgrplus.onm...	Accessed file	globaladmin_zohocorpdmgrplus_onm...	Accessed from "User Photos/Profile P...
	2018-09-26 23:43:27	49.204.208.79	globaladmin@zohocorpdmgrplus.onm...	Accessed file	Upload.aspx	Accessed from "Documents/Forms"
	2018-09-26 23:43:27	49.204.208.79	globaladmin@zohocorpdmgrplus.onm...	Accessed file	EditForm.aspx	Accessed from "Documents/Forms"
	2018-09-26 23:43:27	49.204.208.79	globaladmin@zohocorpdmgrplus.onm...	Accessed file	DisForm.aspx	Accessed from "Documents/Forms"
	2018-09-26 23:24:15	104.47.124.254	app@sharepoint	Accessed file	credit.txt	Accessed from "Documents"
	2018-09-26 21:57:25	49.204.208.79	bhoobalan@zohocorpdmgrplus.onm...	Accessed file	Upload.aspx	Accessed from "Documents/Forms"
	2018-09-26 21:57:25	49.204.208.79	bhoobalan@zohocorpdmgrplus.onm...	Accessed file	EditForm.aspx	Accessed from "Documents/Forms"
	2018-09-26 21:57:25	49.204.208.79	bhoobalan@zohocorpdmgrplus.onm...	Accessed file	DisForm.aspx	Accessed from "Documents/Forms"

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.

O365 Manager Plus

Home Reports Management **Audit** Alerts Monitoring Delegation Settings Support

Search Report (Ctrl+Space)

zohocorpdmgrplus.onmicrosoft.com

Exchange Online

Exchange Activity

Activities by Mailbox Owners

Send As Activities

Activities by Mailbox Non-Owners

Activities by Exchange Admins

Activities by Mailbox Delegates

Mail Move and Delete Activities sent

Mail Contact

Connector

Mailflow

Management Roles

Public Folder

Mailbox Move

Mail Trace

Malware Detection

Spam Detection

DLP Policy Matches

Transport Rule Matches

Mailbox

Mailbox Config

Mailbox Permission

Calendar

Clutter

Azure Active Directory

OneDrive for Business

Microsoft Teams

Period: 27/09/2018 05:16 AM - 27/09/2018 11:11 AM

Business Hours: All Hours

Domains: All Domains

Operations

Count

Create MailboxLogin

Default View: Owner Activity User-Operation Summary

When	Who	Operation	Result	Status	Item	Logon Type	User Type	Client Info	External Access	Target Details	Modified Properties	Folder	Folders	Client
26 Sep 2018 12:44 PM	admin@zohocorpdmgrplus.onmicrosoft.com	MailboxLogin	Succeeded	-	0	0	0	Client=Microsoft.Exchange-Powershell; Microsoft WinRM Client	false	-	-	-	-	Microsoft Exchange
26 Sep 2018 11:13 AM	globalAdmin@zohocorpdmgrplus.onmicrosoft.com	MailboxLogin	Succeeded	-	0	0	0	Client=/owa/SuiteServiceProx.aspx; Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36	false	-	-	-	-	/owa/SuiteService
26 Sep 2018 03:51 AM	globalAdmin@zohocorpdmgrplus.onmicrosoft.com	MailboxLogin	Succeeded	-	0	0	0	Client=Microsoft.Exchange-Powershell; Microsoft WinRM Client	false	-	-	-	-	Microsoft Exchange
26 Sep 2018 02:23 AM	globalAdmin@zohocorpdmgrplus.onmicrosoft.com	MailboxLogin	Succeeded	-	0	0	0	Client=Microsoft.Exchange-Powershell; Microsoft WinRM Client	false	-	-	-	-	Microsoft Exchange

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](#).

User Logon Activity ⓘ

Office 365 Tenant: zohocorpdmgrplus.onmicrosoft.com

Period: 27/08/2018 04:24 AM - 27/09/2018 11:11 AM

Business Hours: All Hours

Generate Now

Generated on: 26 Sep 2018 08:00 AM

When	Who	Client IP	Result Status	Reason	Operation	Client	Record Type
26 Sep 2018 08:38 PM	o365-demo@zohocorpdmgrplus.onmicrosoft.com	202.58.11.236	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 08:38 PM	balaa@zohocorpdmgrplus.onmicrosoft.com	121.244.91.2	Failed	Details	UserLoginFailed	-	15
26 Sep 2018 08:31 PM	o365team@zohocorpdmgrplus.onmicrosoft.com	121.244.91.2	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 08:20 PM	o365team@zohocorpdmgrplus.onmicrosoft.com	182.74.243.57	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 08:16 PM	Sync_OHP-WSM_f8e6869d6ce6@zohocorpdmgrplus.onmicrosoft.com	122.15.156.138	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 08:15 PM	Sync_OHP-WSM_f8e6869d6ce6@zohocorpdmgrplus.onmicrosoft.com	122.15.156.138	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 08:13 PM	validation@zohocorpdmgrplus.onmicrosoft.com	121.244.91.2	Failed	Details	UserLoginFailed	-	15
26 Sep 2018 08:05 PM	balaa@zohocorpdmgrplus.onmicrosoft.com	121.244.91.2	Failed	Details	UserLoginFailed	-	15
26 Sep 2018 08:01 PM	o365team@zohocorpdmgrplus.onmicrosoft.com	121.244.91.2	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 07:58 PM	o365-demo@zohocorpdmgrplus.onmicrosoft.com	202.58.11.236	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 07:50 PM	o365team@zohocorpdmgrplus.onmicrosoft.com	182.74.243.57	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 07:47 PM	log360demo@zohocorpdmgrplus.onmicrosoft.com	117.20.43.11	Failed	Details	UserLoginFailed	-	15
26 Sep 2018 07:46 PM	Sync_OHP-WSM_f8e6869d6ce6@zohocorpdmgrplus.onmicrosoft.com	122.15.156.138	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 07:45 PM	Sync_OHP-WSM_f8e6869d6ce6@zohocorpdmgrplus.onmicrosoft.com	122.15.156.138	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 07:35 PM	o365team@zohocorpdmgrplus.onmicrosoft.com	121.244.91.2	Succeeded	Details	UserLoggedIn	-	15
26 Sep 2018 07:35 PM	balaa@zohocorpdmgrplus.onmicrosoft.com	121.244.91.2	Failed	Details	UserLoginFailed	-	15

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.

Exchange Admin Activity

Office 365 Tenant: zohocorpdmgrplus.onmicrosoft.com

Period: 27/08/2018 04:26 AM - 27/09/2018 11:13 AM

Business Hours: All Hours

Generate Now

Generated on: 10 Aug 2016 11:33 AM

When	Activity	Who	Object Modified	Succeeded	Full Command
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee satishtest3@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee satishtest4@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee shared16641@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee sharedexchangembx1@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee sharedexchangembx2@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee sharedtest003@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee sharedtest001@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee spk1@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee sharedtest@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee temp@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee test@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee testroom@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee testroom@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:47 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee testroom@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:46 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee testshared1111@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:46 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee upn-value1@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com
26 Sep 2018 03:46 AM	Add-RecipientPermission	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	abcMailBox10096	true	Add-RecipientPermission -Trustee cse202@zohocorpdmgrplus.onmicrosoft.com -Confirm False -AccessRights SendAs -Identity abcMailBox10096@zohocorpdmgrplus.onmicrosoft.com

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.

OneDrive Events Log

Office 365 Tenant: zohocorpdmgrplus.onmicrosoft.com

Period: 27/08/2018 04:27 AM - 27/09/2018 11:13 AM

Business Hours: All Hours

Generate Now

Generated on: 10 Aug 2016 11:32 AM

When	Activity	Who	Source Relative URL	Source file name	Destination Relative URL	File URL	Record
26 Sep 2018 01:49 PM	FileAccessed	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	Documents	Credit.docx	-	https://zohocorpdmgrplus-my.sharepoint.com/personal/bhoobalan_zohocorpdmgrplus_onmicrosoft_com/documents/credit.docx	6
26 Sep 2018 01:11 PM	FileUploaded	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	Documents/TestFolder	2018-09-26T20_10_37_00_00	-	https://zohocorpdmgrplus-my.sharepoint.com/personal/bhoobalan_zohocorpdmgrplus_onmicrosoft_com/documents/testfolder/2018-09-26T20_10_37_00_00	6
26 Sep 2018 01:09 PM	FileAccessed	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	Documents	Credit.docx	-	https://zohocorpdmgrplus-my.sharepoint.com/personal/bhoobalan_zohocorpdmgrplus_onmicrosoft_com/documents/credit.docx	6
26 Sep 2018 11:17 AM	FileUploaded	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	Documents/TestFolder	2018-09-26T18_16_57_00_00	-	https://zohocorpdmgrplus-my.sharepoint.com/personal/bhoobalan_zohocorpdmgrplus_onmicrosoft_com/documents/testfolder/2018-09-26T18_16_57_00_00	6
26 Sep 2018 11:17 AM	FileUploaded	bhoobalan@zohocorpdmgrplus.onmicrosoft.com	Documents/TestFolder	2018-09-26T18_16_59_00_00	-	https://zohocorpdmgrplus-my.sharepoint.com/personal/bhoobalan_zohocorpdmgrplus_onmicrosoft_com/documents/testfolder/2018-09-26T18_16_59_00_00	6
26 Sep 2018 11:13 AM	FileAccessed	globaladmin@zohocorpdmgrplus.onmicrosoft.com	Documents	Document.docx	-	https://zohocorpdmgrplus-my.sharepoint.com/personal/globaladmin_zohocorpdmgrplus_onmicrosoft_com/documents/document.docx	6
26 Sep 2018 11:13 AM	FileAccessed	globaladmin@zohocorpdmgrplus.onmicrosoft.com	User Photos/Profile Pictures	globaladmin_zohocorpdmgrplus_onmicrosoft_com_STHumb.jpg	-	https://zohocorpdmgrplus-my.sharepoint.com/user/photos/profile/pictures/globaladmin_zohocorpdmgrplus_onmicrosoft_com_stthumb.jpg	6

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.

Mail Traffic Policy Match Summary

Office 365 Tenant: zshocorpadmgrplus.onmicrosoft.com

Period: 20/08/2017 06:28 AM - 21/09/2017 06:28 AM

Generate Now

Generated on: 01 Nov 2016 06:47 AM

Date(GMT)	Direction	Domain	Event Type	Message Count	DLP Policy	Transport Rule	Action
31 Oct 2016	Inbound	Organization Level	TransportRuleActionHits	1	-	AllMail	ApplyHtmlDisclaimer
31 Oct 2016	Inbound	Organization Level	TransportRuleHits	1	-	AllMail	SetAuditSeverityLow
30 Oct 2016	Inbound	Organization Level	TransportRuleHits	5	-	AllMail	SetAuditSeverityLow
30 Oct 2016	Inbound	Organization Level	TransportRuleActionHits	5	-	AllMail	ApplyHtmlDisclaimer
29 Oct 2016	Inbound	Organization Level	TransportRuleHits	2	-	AllMail	SetAuditSeverityLow
29 Oct 2016	Inbound	Organization Level	TransportRuleActionHits	2	-	AllMail	ApplyHtmlDisclaimer
29 Oct 2016	Outbound	Organization Level	TransportRuleActionHits	1	-	AllMail	ApplyHtmlDisclaimer
29 Oct 2016	Outbound	Organization Level	TransportRuleHits	1	-	AllMail	SetAuditSeverityLow
28 Oct 2016	Inbound	Organization Level	TransportRuleActionHits	4	-	AllMail	ApplyHtmlDisclaimer
28 Oct 2016	Inbound	Organization Level	TransportRuleHits	4	-	AllMail	SetAuditSeverityLow
28 Oct 2016	Outbound	Organization Level	TransportRuleHits	1	-	AllMail	SetAuditSeverityLow
28 Oct 2016	Outbound	Organization Level	TransportRuleActionHits	1	-	AllMail	ApplyHtmlDisclaimer
27 Oct 2016	Inbound	Organization Level	TransportRuleActionHits	6	-	AllMail	ApplyHtmlDisclaimer
27 Oct 2016	Inbound	Organization Level	TransportRuleHits	6	-	AllMail	SetAuditSeverityLow
26 Oct 2016	Outbound	Organization Level	DLPRuleHits	5	APA	Australia Privacy: Attachment not supported	SetAuditSeverityMedium
26 Oct 2016	Outbound	Organization Level	TransportRuleHits	5	-	Australia Privacy: Attachment not supported	SetAuditSeverityMedium
26 Oct 2016	Inbound	Organization Level	TransportRuleActionHits	8	-	AllMail	ApplyHtmlDisclaimer

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