PCI Compliance
with M365 Manager Plus

About PCI-DSS

Payment Card Industry Data Security Standard (PCI DSS) compliance is adherence to the set of policies and procedures developed to protect credit, debit and cash card transactions and prevent the misuse of cardholders' personal information. PCI DSS compliance is required by all card brands.

The Payment Card Industry Security Standards Council (PCI SSC) develops and manages the PCI standards and associated education and awareness efforts. The PCI SSC is an open global forum, with the five founding credit card companies -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. -- responsible for carrying out the organization's work.

Please note that the efforts and procedures required to establish compliance in each section may vary in different organizations depending on their systems configuration, internal procedures, nature of business, and other factors.

Usage of the below mentioned reports may not guarantee complete organizational compliance. This document can be used as a reference guide for complying with PCI industrial mandate.

PCI-DSS compliance with M365 Manager Plus

To comply with industrial mandates various control methods have to implemented. For management simplicity we have mapped the compliance requirements with the required control methods. You can find the reports required to complete the control methods subsequently. Though mentioned separately, all the control methods are interlinked and often required by most of the regulations.

Access Control

Account Management

User Management

Integrity Monitoring

Credentials Management

Data Governance

Configuration Management

Audit Trail

Requirements	Control Methods
Requirement 3: Protect stored cardholder data	
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes	Data Governance
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	Data Governance
Requirement 5: Use and regularly update anti-virus software or programs	
5.3 Ensure that anti-virus mechanisms are actively running	User Management

and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	
Requirement 6: Develop and maintain secure systems and application	
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Account Management
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	Audit Trail
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls. 6.4.2 Separation of duties between development/test and production environments	Access Control
6.4.4 Removal of test data and accounts from system components before the system becomes active/goes into production.	Account Management
6.4.5.2 Documented change approval by authorized parties	Audit Trail
Requirement 7: Restrict access to cardholder data by business need to know	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Access Control Account Management
7.1.3 Assign access based on individual personnel's job classification and function	Account Management User Management
7.1.4 Require documented approval by authorized parties specifying required privileges.	Account Management
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Access Control Integrity Monitoring
Requirement 8: Assign a unique ID to each person with computer access	
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	Account Management Access Control

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components	User Management
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Account Management Access Control Audit Trail
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	Account Management Credentials Management
8.1.3 Immediately revoke access for any terminated users.	Account Management
8.1.4 Remove/disable inactive user accounts within 90 days.	Account Management
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access.	Account Management Access Control
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	Access Control
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Access Control
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Access Control
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Access Control Credentials Management Configuration Management
8.2.3 Passwords/passphrases require a minimum length of at least seven characters and contain both numeric and alphabetic characters or equivalent parameters are specified. 8.2.4 Change user passwords/passphrases at least once every 90 days. 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	Access Control Credentials Management Configuration Management
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately	Access Control

after the first use.	Credentials Management Configuration Management
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	Access Control Configuration Management
8.5 Do not use group, shared, or generic IDs, passwords.	Access Control Account Management
8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	Access Control Account Management
Requirement 10: Track and monitor all access to network resources and cardholder data	
10.1 Implement audit trails to link all access to system components to each individual user.	Access Control Audit Trail
10.2 Implement automated audit trails for all system components to reconstruct the following events:	Audit Trail
10.2.1 All individual user accesses to cardholder data.	Access Control
10.2.2 All actions taken by any individual with root or administrative privileges.	User Management
10.2.3 Access to all audit trails	Audit Trail
10.2.4 Invalid logical access attempts.	Access Control
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	Access Control User Management

	Account Management
10.2.6 Initialization, stopping, or pausing of the audit logs	Audit Trail
10.2.7 Creation and deletion of system-level objects	Integrity Monitoring
10.3 Record at least the following audit trail entries for all system components for each event: User identification; Type of event; Date and time; Success or failure indication; Origination of event	Audit Trail
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	Configuration Management
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Audit Trail
Requirement 11: Regularly test security systems and processes	
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). 11.3 Implement a methodology for penetration testing	Audit Trail Access Control
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Integrity Monitoring

Control methods and M365 Manager Plus reports

The following section will map the control methods and M365 Manager Plus reports that help to implement them.

Access Control

Microsoft 365 Service	**M365 Manager Plus Reports**
Exchange Online	Exchange Admin Activity Exchange User Activity Non-Owner Mailbox Access Recently Added Members to Groups

	Recently Removed members from groups
	Group Members
	Distribution List Members
	Active Directory
	Reset User Password
	Disabled Exchange Users
	Send-As Permission
	Send-on-Behalf Permission
	Mailbox Permissions Changes
	Permissions Changes
	Unified Messaging Mailbox Policy
	User Rights Assignment Policy Changes
	DLP Policy Matches
	OWA Logon by Users
	OWA Logon by OS
	OWA Logon by Browsers
	Public Folder Activity
Azure Active Directory	Recently Enabled Accounts
	User Account Status Changes
	User Logon Activity
	Temporary User Accounts
	Never Expiring Passwords
	All Users
	Password Expired Users
	Azure Locked Users
	Group Modification Report
	Group Settings Modification Report
	Azure Admin Activity,
	Recently modified users
	Multi Factor Authentication Status

	Reset User Password
	Change User Password
	Update User Credentials
	User Activity(based on Business Hours)
	User Logon Activity
OneDrive for Business	OneDrive Events Log
	OneDrive Files Accessed
	OneDrive File Modifications
	OneDrive Files Renamed
	OneDrive Files Movement
	OneDrive File Operation
	OneDrive Downloads
	OneDrive File Uploads
	OneDrive Deleted Files
	OneDrive Download Sync
	OneDrive Upload Sync
Microsoft Teams	Added Channel
	Created Team
	Deleted Team
	Users Signed in to Teams
	Changed Setting (legacy)
	Changed Organizational Settings
	Changed Team Settings
	Changed Channel Settings
Power BI	Created Dashboard
	Viewed Dashboard
	Modified Dashboard
	Deleted Dashboard
	Printed Dashboard
	Shared Dashboard
	Created Groups
	Added Group members
	Started Pro-trial Subscriptions
	Created Reports
	Viewed Reports
	Modified Reports

	Deleted Reports
	Shared Reports
	Printed Reports
	Downloaded Reports
	Published Reports
	Exported Dashboard Tile
	Exported Reports
	Started Extended Trial
	Admin Portal Activities
	Viewed Usage Metrics
	Analyzed Dataset
	Created Organizational Content Pack
	Deleted Dataset Objects
Sway	Viewed sway
	Enabled and disabled sway
	Enabled and disabled sway service
	Enabled and disabled external sway sharing
	Created, modified, and deleted sway

Account Management

Microsoft 365 Service	M365 Manager Plus Reports
Exchange Online	Non-Owner Mailbox Access
	Contact Audit Log
	Added Member to Group
	Removed Member from Group
	Group Members
	Users Not in Group
	Groups with Disabled Users
	Account Policy Changes
	User Configuration Changes
	Role Assignment policy
	Unified Messaging Mailbox Policy
	User Rights Assignment Policy Changes
	DLP Policy Matches

Azure Active Directory	Recently Enabled Accounts
	Recently Created User Account
	Recently Modified User Account
	Recently Deleted User Account
	Password change Report
	Accounts with Most Logon Activity (In All Logon Activities Report)
	All Users
	Password Expired User Accounts
	Locked User Accounts
	Never Expiring Passwords
	Azure Locked Users
	Azure User Activities
	Recent Logon Failure
	Recent Successful Logon
	User Logon Activtiy
	Exchange User Activity
Micorosft Teams	Added Channel
	Created Team
	Deleted Team
	Users Signed in to Teams
	Changed Setting (legacy)
	Changed Organizational Settings
	Changed Team Settings
	Changed Channel Settings
Power BI	Started Pro-trial Subscriptions
	Started Extended Trial
	Admin Portal Activities
	Viewed Usage Metrics
	Analyzed Dataset
	Created Organizational Content Pack
Sway	Viewed sway
	Enabled and disabled sway
	Enabled and disabled sway service
	Enabled and disabled external sway sharing
	Created, modified, and deleted sway

Credentials Management

Microsoft 365 Service	M365 Manager Plus Reports
Azure Active Directory	Password Change
	Never Expiring Passwords
	Soon to Expire Users
	Password Changed Users
	Password Unchanged Users
	Multi Factor Authentication Status
	Recently Password Reset Users
	Forced Password Change
	Updated User Credentials
Microsoft Teams	Users Signed in to Teams

User Management

Microsoft 365 Service	M365 Manager Plus Reports
Exchange Online	Exchange User Activity
	Mailbox Features
	Mailbox with ForwardTo
	Mailbox Auto Reply Configuration
	Group Members
	Recently Added Users to Groups
	Recently Deleted Users from Groups
	Distribution List Members
	Dynamic Distribution Group Members
	Mailbox Permissions Changes
	Created and deleted Malware Filter Policy
	Created, Modified, and Deleted Phishing Rules
	Created, Modified, and Deleted Role Assignments
	Created, Modified, and Deleted Safe Attachment Policies
	Created, Modified, and Deleted Safe Link Policies
	OWA Logon by Users
	OWA Logon by OS
	OWA Logon by Browsers
Azure Active Directory	Added Users
	Updated Users
	Deleted Users

	Cloud users
	Synced Users
	Never Expiring Passwords
	User Logon Activity
	Added Users to Admin Role
	Recent Logon Failure
	Recent Successful Logon
	User Activity(based on Business Hours)
	User Logon Activity
OneDrive for Business	OneDrive Events Log
	OneDrive Files Accessed
	OneDrive File Modifications
	OneDrive Files Renamed
	OneDrive Files Movement
	OneDrive File Operation
	OneDrive Downloads
	OneDrive File Uploads
	OneDrive Deleted Files
	OneDrive Download Sync
	OneDrive Upload Sync
Microsoft Teams	Added Channel
	Created Team
	Deleted Team
	Users Signed in to Teams
	Changed Setting (legacy)
	Changed Organizational Settings
	Changed Team Settings
	Changed Channel Settings
Sway	Viewed sway
	Enabled and disabled sway
	Enabled and disabled sway service
	Enabled and disabled external sway sharing
	Created, modified, and deleted sway

Integrity Monitoring

Microsoft 365 Service	M365 Manager Plus Reports
Exchange Online	OWA Logon by Users
	OWA Logon by OS
	OWA Logon by Browsers
Azure Active Directory	Recent Logon Failure
	Recent Successful Logon
	User Activity(based on Business Hours)
	User Logon Activity
OneDrive for Business	OneDrive Files Accessed
	OneDrive File Modifications
	OneDrive File Renaming
	OneDrive File Movement
	OneDrive File Operations
	OneDrive Upload
	OneDrive Downloads
	OneDrive Deleted Files
	OneDrive Events Log
Microsoft Teams	Added Channel
	Created Team
	Deleted Team
	Users Signed in to Teams
	Changed Setting (legacy)
	Changed Organizational Settings
	Changed Team Settings
	Changed Channel Settings
Power BI	Created Dashboard
	Viewed Dashboard
	Modified Dashboard
	Deleted Dashboard
	Printed Dashboard
	Shared Dashboard
	Created Groups
	Added Group members
	Started Pro-trial Subscriptions
	Created Reports
	Viewed Reports

	Modified Reports
	Deleted Reports
	Shared Reports
	Printed Reports
	Downloaded Reports
	Published Reports
	Exported Dashboard Tile
	Exported Reports
	Started Extended Trial
	Admin Portal Activities
	Viewed Usage Metrics
	Analyzed Dataset
	Created Organizational Content Pack
	Deleted Dataset Objects
Sway	Viewed sway
	Enabled and disabled sway
	Enabled and disabled sway service
	Enabled and disabled external sway sharing
	Created, modified, and deleted sway

Data Governance

Microsoft 365 Service	M365 Manager Plus Reports
Exchange Online	Exchange Online Mailbox Permissions Changes
	Added and deleted folder level permissions
	Added and deleted send-as permissions
	Added and deleted mailbox permissions
	Configured permissions for folders within user mailbox
	Exchange Online Mailbox Policy Changes
	Created, modified, and deleted UM mailbox policies
	Transport rule matches
	Messages that triggered transport rules
	Folder Message Count and Size
	Attachment by File Size
	Message by Subject
	Mailbox Message Restrictions
	Mailbox Clutter Details
	OWA Attachment Policies

	OWA Attachment Policy by Users
OneDrive for Business	OneDrive Files Accessed
	OneDrive File Modifications
	OneDrive File Renaming
	OneDrive File Movement
	OneDrive File Operations
	OneDrive Upload
	OneDrive Downloads
	OneDrive Deleted Files
	OneDrive Events Log
	Checked-in and checked-out file
	Discarded file check-out
Power BI	Created Dashboard
	Viewed Dashboard
	Modified Dashboard
	Deleted Dashboard
	Printed Dashboard
	Shared Dashboard
	Created Groups
	Added Group members
	Created Reports
	Viewed Reports
	Modified Reports
	Deleted Reports
	Shared Reports
	Printed Reports
	Downloaded Reports
	Published Reports
	Exported Dashboard Tile
	Exported Reports
	Viewed Usage Metrics
	Analyzed Dataset
	Deleted Dataset Objects
Sway	Viewed sway
	Enabled and disabled sway
	Enabled and disabled sway service
	Enabled and disabled external sway sharing
	Created, modified, and deleted sway

Configuration Management

Microsoft 365 Service	M365 Manager Plus Reports
Exchange Online	Created and deleted mailboxes
	Recovered soft deleted mailboxes
	Created, suspended, and resumed mailbox restore requests
	Configured mailbox settings
	Created mailboxes for existing users
	Disabled mailboxes of existing users
	Configured junk email rule for specific mailboxes
	Modified CAS settings in a mailbox
	Mailbox Sizes
	Mailbox Size Restrictions
	Current Mailbox Size vs Quota
	Archive Mailbox Sizes
	Mailbox Storage Information
	Mailbox Size Over Time
	Created management role assignments
	Modified management role assignments
	Deleted management role assignments
	Created and deleted management role groups
	Added and deleted management role group members
	Modified role groups
	Updated role groups
	Added and deleted folder level permissions
	Added and deleted send-as permissions
	Added and deleted mailbox permissions
	Configured permissions for folders within user mailbox
	Account Permissions
	Group Policy Object Delegation
	Email Address Policy Changes
	Exchange Online Mailbox Policy Changes
	New, rotated, and modified DKIM signing policies
Microsoft Teams	Changed Setting (legacy)
	Changed Organizational Settings
	Changed Team Settings
	Changed Channel Settings

Power BI	Started Pro-trial Subscriptions
	Started Extended Trial
	Admin Portal Activities
	Viewed Usage Metrics
	Analyzed Dataset
	Created Organizational Content Pack
Sway	Enabled and disabled sway
	Enabled and disabled sway service
	Enabled and disabled external sway sharing

Audit Trail

Microsoft 365 Service	M365 Manager Plus Reports
Exchange Online	Created and deleted mailboxes
	Recovered soft deleted mailboxes
	Created, suspended, and resumed mailbox restore requests
	Configured mailbox settings
	Created mailboxes for existing users
	Disabled mailboxes of existing users
	Created, modified, and deleted Microsoft 365 groups
	Created, modified, and deleted dynamic distribution groups
	Created, modified, and deleted distribution groups
	Added and replaced distribution group members
	Deleted unified groups and unified group links
	Added members, owners, and subscribers to groups
	Created, modified, and deleted email users
	Modified user attributes
	Modified linked user account properties
	Purged messages from mailbox
	Deleted messages form Deleted Items folder
	Moved messages to Deleted Items folder
	Moved messages to another folder
	Created or received messages
	Sent messages using send-on behalf permission
	Copied message to another folder
	Users signed into mailbox
	Sent messages using SendAs permission
	Enabled or disabled focused inbox for mailboxes

	Enabled/disabled UM call answering rules
	Created, modified, and deleted call answering rules
	Created, modified and tested site mailboxes
	Synchronisation triggered site mailboxes
	Created and modified site mailbox provisioning policies
	Added, modified, and deleted management role entry
	Updated and deleted hybrid configurations
	Configured message flow settings
	Created, modified, and deleted OnPremisesOrganization objects
	Enabled and disabled UM auto attendants
	Created, modified, and deleted auto attendants
	Transport rule matches
	Messages that triggered transport rules
	Created, modified and deleted malware filter rules
	Created, modified, and deleted malware filter policies
	Created, validated, and deleted inbound connectors
	Created, validated, and deleted outbound connectors
	Created, modified, and deleted intra organization connectors
	Created, modified, and deleted UM dial plans
	Created, modified, and deleted management role assignments
	Created, modified, and deleted public folder migration requests
	Resumed and suspended public folder migration requests
	Resumed and suspended public folder mailbox migration requests
	Enabled and disabled UM IP gateway
	Created, modified, and deleted UM IP gateway configurations
	Configured auto reply settings for a mailbox
	Created mailbox folders
	Configured publishing or sharing settings on a calendar folder
	Messages with no delivery status
	Messages undelivered or filtered as spam/malware
	Messages yet to be delivered
	Successfully delivered messages
	Messages undelivered due to expanded group membership
	Created, modified, and deleted role assignment policies
	Modified transport configuration settings

	Removed text messaging settings
	Compared verification codes
	Verification codes sent to users' mobile phone
	Text messaging notifications configured
	PINs reset for UM mailbox
	Modified existing accepted domains
	Created, modified, and deleted sharing policies
	Created, modified, Tested, and deleted organization relationships
	Created and deleted availability address space objects
	Modified access level for free/busy information
	Created, and deleted availability configurations
	Created, modified, and deleted OWA mailbox policies
	Modified mailbox message configuration
	Modified mailbox message configuration
	Modified wen spelling checker options
	Calendar settings applied for users using OWA calendars
	Modified S/MIME configuration
	New and deleted hotmail, POP or IMAP subscriptions
	Created and modified POP subscriptions
	Created, and modified IMAP subscriptions
	Created and modified hotmail subscriptions
	Created, modified, and deleted contact integration subscription
	Activity alerts in Security & Compliance center
	Created, modified, and deleted safe link policies
	Enabled and disabled safe link policies
	Created, modified, and deleted safe attachment rules
	Enabled and disabled safe attachment rules
	Created, and deleted safe attachment policies
	New phish filter policy configured
	Imported and exported UM prompts
	Messages marked as malware
	Spam filtered by advanced filters
	Messaged filtered as bulk mail
	Messages filtered based on content
	Messages filtered by transport rule
	Messages from blocked users
	Messages filtered by content, rules or other configuration
	Messages addressed to an unknown recipient

	Messages blocked based on SMTP
	Messages blocked based on sender IP
	Created and deleted public folder sync
	Created, modified, and deleted partner app configurations
	Tested OAuth authentication
	Modified, and deleted user photos
	Enabled and disabled UM for mailboxes
	Modified UM mailbox properties
	Imported contacts to Exchange Online mailboxes
	Created email messages
	Tested MAPI connectivity
	Enabled and disabled apps for a specific user
	Created and deleted apps
	Modified availability of organization apps
	Modified mailbox plans
	Exchange organisation settings configured
	Enabled organization customization
	Modified gateway server IP addresses
	Created and deleted remote domains
	Connections configured for a remote domain
	Configured text message notification for calendar events
	Modified calendar processing options for resource mailboxes
	Created, modified, and deleted inbox rules
	Enabled and disabled inbox rules
	Configured junk email rule for specific mailboxes
	Configured Exchange ActiveSync settings
	Mobile device mailbox policy settings applied to server
	Configured and deleted device access level for rules
	Created and deleted active sync mailbox policies
	Created and deleted active sync device access rule
	Created, modified, and deleted mobile device mailbox policies
	Deleted data from mobile device
	Deleted mobile devices
	Created, modified, and deleted UM mailbox policies
	Added and deleted folder level permissions
	Added and deleted send-as permissions
	Added and deleted mailbox permissions
	Configured permissions for folders within user mailbox

	Modified CAS settings in a mailbox
	Configured federated organization identifier
	New federation trust set up
	Created and deleted public folder
	Hierarchy updated public folders
	Mail enbled and disabled public folders
	Added and deleted permissions to public folders
	Modified mail enabled public folders
Security	Messages filtered by DLP rule
	Messages incorrectly filtered by DLP rule
	Messages that override one or more DLP rules
	Messages that triggered DLP rules and policy rules
	Created and deleted UM hunt group
	Created, modified, and deleted management scopes
	Created, modified, and deleted content filter policies
	Released quarantine messages
	Created, modified, and deleted connection filter policies
	Created, modified, and deleted content filter rules
	Enabled and disabled content filter rules
	Modified outbound spam filter policy
	New, rotated, and modified DKIM signing policies
	Created and deleted management role groups
	Added and deleted management role group members
	Modified role groups
	Updated role groups
	Created, modified, and deleted email contacts
	Configured clutter settings for mailboxes
	Created and deleted management roles
	Deleted migration users
	Tested migration server availability
	Exported migration reports
	Modified staged IMAP, and remote migrations
	Created and deleted migration endpoints
	Started and stopped batch migration process
	Created, finalized, and deleted migration batches
	Created, modified, resumed, suspended, and deleted move requests
	Updated migration requests

Azure Active Directory	Added, updated, and deleted user
	Updated and deleted group
	Created group settings
	Added and removed member from a group
	Set license properties
	Changed user license
	Added users to admin role
	Deleted users from member role
	Updated company contact information
	Sign-in using password
	Sign-in using cookies
	Successful and failed logins
	Added modified, and removed delegation entry
	Added and removed service principals
	Added and removed credentials of service principals
	Reset user password
	Changed user password
	Set property that forces user to change password
	Updated user credentials
OneDrive for Business	Allowed and blocked computers from syncing files
	Downloaded and uploaded files
	Downloaded and uploaded file changes
	Created, accepted and withdrawn sharing invitations
	Created, used, and deleted company-wide share links
	Shared and unshared file, folder or site
	Created, accepted and denied access requests
	Created, used, and deleted anonymous links
	Renamed file
	Moved file
	Modified file
	Uploaded and downloaded file
	Deleted file
	Restored file
	Checked-in and checked-out file
	Discarded file check-out
	Copied file
	Accessed file
Sway	Viewed sway

	Enabled and disabled sway
	Enabled and disabled sway service
	Enabled and disabled external sway sharing
	Created, modified, and deleted sway
Microsoft Teams	Added Channel
	Created Team
	Deleted Team
	Users Signed in to Teams
	Changed Setting (legacy)
	Changed Organizational Settings
	Changed Team Settings
	Changed Channel Settings
Power BI	Created Dashboard
	Viewed Dashboard
	Modified Dashboard
	Deleted Dashboard
	Printed Dashboard
	Shared Dashboard
	Created Groups
	Added Group members
	Started Pro-trial Subscriptions
	Created Reports
	Viewed Reports
	Modified Reports
	Deleted Reports
	Shared Reports
	Printed Reports
	Downloaded Reports
	Published Reports
	Exported Dashboard Tile
	Exported Reports
	Started Extended Trial
	Admin Portal Activities
	Viewed Usage Metrics
	Analyzed Dataset
	Created Organizational Content Pack
	Deleted Dataset Objects

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**