

Beyond native tools: Advanced Microsoft 365 auditing, reporting, and automation



I. Introduction

Simplifying Microsoft 365 management

Microsoft 365 has become a must-have for many businesses, making communication, collaboration, and getting work done easier than ever. Microsoft 365 is typically the core part of everyday work, from emails and document management to team collaboration. But as organizations grow and depend more on these tools, it becomes harder to keep everything working well, securely, and simply.

Ensuring peak performance, enforcing strong security measures, and simplifying administrative tasks demands considerable time, specialized expertise, and the right set of tools. Solutions that augment and complement Microsoft 365's native management features are becoming more prominent. They help IT professionals manage their Microsoft 365 environments better.

Part 1: Where Microsoft 365 administration often falls short

Microsoft 365 provides a range of administrative tools. However, these tools often fall short of meeting the complex demands of modern organizational structures and the need for granular control. In this section, we delve into the key limitations of native Microsoft 365 management capabilities.

1.1 Challenges in managing Microsoft 365 Groups

Microsoft 365 Groups are designed to enhance team collaboration. However, their management can present several challenges for IT administrators. By default, Microsoft 365 allows any user to create groups. While this can foster teamwork and flexibility, it can also lead to a rapid proliferation of groups, many of which may be redundant, inactive, poorly managed, or lack clear ownership.

This "group sprawl" increases administrative overhead, complicates governance, makes it difficult for users to find relevant groups, and consumes valuable resources (e.g., storage and licenses). In very large groups, especially those with over 1,000 members, users may experience performance degradation when accessing group resources. This can manifest as delays when accessing group calendars, conversations, files, and other shared resources in Outlook, Teams, and other applications. These performance bottlenecks can hinder real-time collaboration, reduce user productivity, and negatively impact the overall user experience.

The primary management tools within Microsoft 365, namely the Microsoft 365 admin center and PowerShell scripts, often lack intuitive and efficient bulk operation capabilities. Tasks such as adding or removing members, updating group settings, configuring group policies, and managing group life cycles (creation, modification, deletion) can be time-consuming and complex, especially in organizations with a large number of groups.

PowerShell, while powerful, requires specialized scripting knowledge, which may not be readily available to all IT administrators. Native Microsoft 365 tools also provide limited capabilities for enforcing consistent group naming conventions, access policies, life cycle management policies, and compliance requirements. This can result in a fragmented and inconsistent group landscape, making it difficult to maintain control, enforce security policies, track group usage, and ensure compliance with organizational standards and regulatory requirements.

1.2 Deficiencies in security auditing and alerting

Maintaining the security of a Microsoft 365 environment requires robust auditing capabilities to track user activity, detect potential security threats, and ensure compliance with regulatory mandates. However, native Microsoft 365 auditing tools have certain limitations.

Microsoft 365 provides basic auditing functionality through Microsoft 365 audit logs, which consolidate logs from various services. While these logs record a wide range of activities, they may not always capture the specific details needed for in-depth security analysis, forensic investigations, or compliance monitoring. For example, detailed information about specific file access events, changes to sensitive data, or granular user actions within applications may not be consistently logged or easily accessible.

The sheer volume of audit data generated in a typical Microsoft 365 environment can also be overwhelming. The built-in tools often lack advanced features for filtering, searching, correlating, and analyzing audit data, making it a time-consuming and complex process to investigate security incidents, identify patterns of suspicious activity, and perform comprehensive forensic analysis.

Administrators may struggle to extract meaningful insights from the vast amount of raw log data. Native Microsoft 365 auditing tools primarily focus on log storage and retrieval. They lack real-time analysis capabilities to detect and alert on suspicious activity as it occurs. This can delay the incident response, increase the dwell time of attackers within the environment, and increase the potential for damage and data loss.

Additionally, Microsoft 365's audit log retention policies may not meet the long-term data retention requirements of all organizations, particularly those in highly regulated industries. This can pose challenges for compliance, historical analysis, and legal discovery purposes. Organizations may need to implement additional logging solutions to meet their specific retention needs.

Effective alerting is crucial for proactively identifying and responding to security threats, service disruptions, and other critical events. However, the alert features in the Microsoft 365 admin center have certain shortcomings. Native Microsoft 365 alerts often provide limited customization options; administrators may not be able to define highly specific alert rules, customize alert thresholds, specify granular alert conditions, or tailor alert messages to meet their specific monitoring needs.

This lack of customization can lead to alert fatigue, where administrators are inundated with a large volume of generic or low-priority alerts. This can desensitize them to important notifications, increasing the risk of missing critical security incidents or service disruptions.

Alerts generated by native Microsoft 365 tools often lack sufficient context and enrichment. This can make it difficult for administrators to quickly understand the severity and scope of the issue, prioritize response efforts, and take appropriate action. Furthermore, alert notifications may not always be delivered in real time or through preferred communication channels. Delays in receiving critical alerts can increase the time it takes to respond to incidents, potentially allowing security threats to spread or service disruptions to impact more users.

1.3 Complex administration of RBAC

Managing administrative access in Microsoft 365 is essential for maintaining security and ensuring proper control over the environment. Microsoft 365 employs role-based access control (RBAC) to manage permissions. However, native RBAC administration can be complex. While Microsoft 365 offers pre-defined admin roles, these roles can sometimes be too broad, granting more permissions than necessary for specific tasks.

Creating highly granular custom roles using native tools can be complex and time-consuming. Over time, users might accumulate excessive permissions, especially if roles are assigned without frequent review. This permission creep increases the attack surface and the potential for unauthorized access.

A centralized view of all assigned roles and their associated permissions across the entire Microsoft 365 environment is often lacking. This makes it challenging to maintain compliance and conduct access reviews. Moreover, delegating specific administrative tasks, such as password resets or user management, to help desk staff without granting them full admin privileges can be difficult using the standard Microsoft 365 admin center.

1.4 Inefficient user and license management

Managing users and licenses is a fundamental aspect of Microsoft 365 administration. Native tools, however, have certain limitations. The Microsoft 365 admin center often lacks intuitive and efficient capabilities for performing bulk user management tasks.

Creating multiple user accounts, assigning licenses to large groups, managing group memberships, updating user attributes, and performing other common operations can be time-consuming and prone to errors when done manually, one user at a time. While PowerShell can be used to perform bulk operations, it requires specialized scripting knowledge, which some IT administrators may not have. This creates a reliance on skilled scripting experts and increases administrative overhead.

The standard Microsoft 365 admin center provides limited automation features for repetitive tasks. Activities such as password resets, user onboarding and offboarding, scheduled reporting, and other routine administration tasks often require manual intervention, increasing administrative workload and the potential for errors.

Gaining a clear and comprehensive view of license utilization can also be challenging. Identifying unused licenses, optimizing license assignments, tracking license consumption by department or user group, and generating detailed license utilization reports can be difficult with native tools. This lack of visibility can lead to inefficient license management, increased software costs, and potential compliance issues.

1.5 Inadequate reporting and analytics

Obtaining a clear understanding of Microsoft 365 usage patterns, service health, and security posture requires comprehensive and flexible reporting and analytics capabilities. However, native Microsoft 365 tools have certain limitations. The standard Microsoft 365 admin center provides a limited set of pre-built reports, approximately 25, that cover basic usage metrics and service health. These reports often lack the depth, granularity, and customization options needed to address specific reporting requirements.

Administrators have limited ability to customize existing reports or create new reports that align with their organization's unique reporting needs. This can make it difficult to gather the specific data needed for analysis, decision-making, and compliance reporting. Gathering data from different Microsoft 365 services (e.g., Exchange Online, SharePoint Online, Microsoft Teams) often requires navigating multiple admin centers, exporting data from different sources, and manually aggregating the information. However, this fragmented approach can be time-consuming, complex, and prone to errors.

Native Microsoft 365 tools offer limited interactive dashboards with real-time visualizations that provide a consolidated view of key performance indicators (KPIs) and service health metrics. This can hinder administrators' ability to quickly identify trends, detect anomalies, and make informed decisions.

Adding to that, generating reports specifically designed to demonstrate compliance with industry regulations and security standards (e.g., HIPAA, SOX, GDPR) can be challenging with native tools, often requiring manual data collection and report creation.

1.6 Deficient health monitoring and alerting

Maintaining a healthy and smoothly functioning Microsoft 365 environment relies on effective monitoring and alerting capabilities. However, native Microsoft 365 tools have certain limitations. Microsoft 365's built-in service health monitoring features often provide a high-level overview of service availability but may not offer the granular visibility needed to detect and diagnose performance issues at the application or component level.

Native tools may not provide real-time or proactive monitoring capabilities that can detect subtle performance degradation, potential bottlenecks, or emerging issues before they significantly impact users. The alerting mechanisms in Microsoft 365 may lack the customization options needed to define specific thresholds, alert on specific events, or configure granular notification settings. This can increase the risk of alert fatigue or missed critical issues.

In some cases, administrators may be required to manually check service health dashboards or logs to obtain the latest status information. This manual effort can be time-consuming and may delay incident response times.

Part 2: How ManageEngine AD360 addresses these limitations

Solutions designed for Microsoft 365 management like ManageEngine AD360 can extend the capabilities of the native Microsoft 365 admin center and address the limitations outlined above. AD360 provides a wide range of features to simplify administration, enhance security, and improve overall management of the Microsoft 365 environment.

2.1 Enhanced Microsoft 365 Groups Management

When we look at managing Microsoft 365 Groups, AD360 offers a more streamlined approach than the native tools. It really simplifies key administrative tasks like group creation and member management through some well-designed features that enhance efficiency.

A significant benefit comes from its strong bulk management capabilities. This allows administrators to perform actions such as adding or removing members across numerous groups simultaneously, as well as updating group settings en masse. This can noticeably reduce the administrative overhead compared to the standard interface or scripting with PowerShell.

Furthermore, AD360 provides management templates that can help standardize the group creation process and potentially guide naming conventions for better organization. These templates help administrators in standardizing the values and also customizing, as per their organizational policies, the way in which all the user objects should be created or modified.

2.2 Enhanced security auditing and alerting

AD360 is designed to provide advanced auditing, alerting, and security features to help organizations proactively manage security, detect threats, and ensure compliance. It offers comprehensive auditing capabilities with a wide range of pre-built audit reports. It captures granular details about user activities and system changes across various Microsoft 365 services, including Exchange Online, Entra ID, OneDrive for Business, SharePoint Online, and Microsoft Teams.

AD360 provides a large number of predefined audit reports and supports custom audit profiles. Real-time auditing ensures audit logs are constantly updated. It also offers robust real-time alerting features that notify administrators of critical events and potential security threats as they occur. It includes preconfigured alert profiles for common security scenarios, and administrators can customize alert settings, including defining specific alert conditions, setting alert thresholds, customizing alert messages, and configuring alert delivery channels. For example, alerts can be generated for unusual logon attempts, failed logon attempts, unauthorized access, mass file downloads, changes to security settings, suspicious email activity, and DLP policy matches.

AD360 includes advanced content search capabilities that go beyond the basic search functionality provided by Microsoft 365's eDiscovery tools. Administrators can perform granular searches across mailboxes to find emails containing specific keywords, patterns, or sensitive information, such as Social Security numbers, credit card numbers, personal health information, and confidential business data. This feature is valuable for investigating potential data leaks, responding to legal discovery requests, ensuring compliance with data privacy regulations, and proactively detecting phishing attacks.

AD360 also allows administrators to delegate specific security-related tasks to other users without granting them full administrative rights. For example, help desk staff can be granted permissions to reset user passwords, unlock accounts, or block users. Additionally, it often has a geolocation option for audit reports and alert triggers, enabling administrators to track the country from where an action has been performed.

2.3 Simplified RBAC

AD360 simplifies administration through RBAC and templates. It allows administrators to define custom roles with granular permissions, enabling secure delegation of tasks to help desk staff or other support personnel without granting them full administrative rights. Templates simplify many routine management tasks. Templates may be created for changes to users, contacts, mailboxes, and licensing, improving consistency and streamlining routine management actions.

2.4 Streamlined user and license management

AD360 simplifies user and license management with powerful bulk operation capabilities and automation features. It allows administrators to perform various user management tasks in bulk, saving significant time and effort. These tasks include resetting user passwords, blocking or unblocking user accounts, deleting or restoring user accounts, modifying user attributes, creating and managing user groups, and managing external contacts in bulk.

AD360 also provides efficient tools for assigning, removing, and modifying Microsoft 365 licenses for large numbers of users. This includes assigning licenses to multiple users at once, removing licenses from users who no longer require them, changing license types, and generating reports on license usage. Furthermore, it automates various routine administrative tasks to reduce manual effort and improve efficiency. This includes scheduling report generation and distribution, automating user provisioning and de-provisioning, automating password resets, automating group membership management, and creating and enforcing automation policies.

AD360 also provides insights into license utilization, helping organizations optimize their license usage and reduce software costs by identifying unused licenses, tracking license consumption, providing recommendations for reallocating or reclaiming licenses, and generating detailed license utilization reports.

2.5 Enhanced reporting and analytics

AD360 offers a vastly improved reporting and analytics experience compared to native tools, giving IT administrators much greater visibility. It provides a library of hundreds of ready-to-use reports, a significant expansion from the limited set offered by Microsoft 365. These reports offer granular visibility across key Microsoft 365 services, including Exchange Online, Microsoft Entra ID, OneDrive for Business, Teams, SharePoint Online, Yammer, and Microsoft Purview.

Administrators can customize reports to meet their specific needs. This includes filtering report data, selecting specific columns, sorting data, grouping data, and saving customized report configurations. AD360 also automates report generation and distribution. Reports can be scheduled to run automatically on a regular basis and exported in various formats, including PDF, CSV, Excel, and HTML. These reports can be automatically emailed to designated recipients, ensuring that the right people have access to the latest information without manual intervention.

Furthermore, AD360 offers customizable dashboards that provide a consolidated, graphical view of key Microsoft 365 metrics, such as email traffic, user activity, and service health. Dashboards or individual widgets can be embedded into other web pages, portals, or monitoring systems, allowing administrators to access critical information from a centralized location. AD360 also includes pre-built reports designed to assist organizations in meeting the reporting requirements of various IT compliance regulations and security standards, such as HIPAA, SOX, the PCI DSS, the GDPR, ISO 27001, and FISMA.

AD360 also provides reports focused on spam and malware detection. These reports give a comprehensive overview of incoming and outgoing spam and malware activity in the Exchange Online environment, including details on messages identified as spam, content blocked due to spam or malware, senders or domains blocked by administrators, recipients targeted by spam or malware campaigns, and types of malware detected.

This detailed information enables administrators to assess the organization's email security risk, identify trends in spam and malware attacks, evaluate the effectiveness of existing email security policies, make informed decisions about email security configurations, and demonstrate compliance with regulatory requirements related to email security. It also provides reports focused on Exchange Administrator activity, Azure Administrator activity, and holds on mailboxes.

The following table provides a more detailed comparison of the reporting capabilities in native Microsoft 365 versus AD360:

Feature	Native Microsoft 365 Reporting	AD360
Number of pre-built reports	Approximately 25	700+
Report scope	Limited usage and service health metrics	Comprehensive coverage across all major Microsoft 365 services (Exchange Online, Entra ID, OneDrive for Business, Teams, SharePoint Online, Yammer), security, and compliance.
Report customization	Limited	Extensive options: Filtering, column selection, sorting, grouping, custom formulas, calculated columns, report templates, saved configurations.
Report scheduling	Limited	Automated report generation and distribution on flexible schedules (hourly, daily, weekly, monthly).
Report formats	Limited (e.g., CSV, Excel)	Wide range: PDF, CSV, Excel (XLSX), HTML, XML, text, database.
Report delivery	Manual download or online viewing	Automatic delivery via email, network share, FTP, or integration with other systems.
Real-time dashboards	Limited service health dashboards	Customizable dashboards with interactive charts and widgets displaying real-time metrics, trend analysis, and performance indicators.
Compliance reporting	Limited reports; may require manual compilation	Dedicated reports designed for specific regulations (HIPAA, SOX, PCI DSS, the GDPR, ISO 27001, FISMA) with pre-defined views of relevant data.

Historical data	Limited retention policies	Configurable retention policies; ability to retain audit and report data for extended periods to meet compliance and analysis needs.
Aggregation	Limited	Ability to aggregate data across multiple services or time periods; aggregate data to improve readability and analysis.
Trending	Limited	Track performance over specified periods and compare performance.
Context	Limited	Context to allow you to understand why an event occurred.
Geographic information	Limited	IP addresses provide geolocation data of actions performed by a user to get the location of sign-ins and more.
Filtering	Limited	Fine-grained filtering of report information is available, and administrators can filter by user, date, activity, and custom user preferences.
RBAC	Limited	RBAC options let admins allow custom access to users so they can perform tasks without elevated privilege, preventing over exposure of vital data.
Search	Limited search criteria	Search capabilities that allow for searching based on many conditions, including specific events or patterns.
Automation	Limited	Automate tasks to minimize human intervention and allow resources to focus on other tasks.
Audit types	Limited	More than 450 predefined custom audit capabilities allows administrators to generate the exact auditable report.
Custom reporting	Limited	Users can generate the exact audits needed that are unavailable with predefined reports.
License reporting	Limited	Allows admin view of user license usage and the ability to find and remove unused licenses.
User activity reports	Limited	In-depth analysis of user events and file access.
Support for threat detection	Limited	Leverage geofencing to identify unusual access and other threat protection functionality.

2.6 Proactive monitoring and alerting

AD360 enhances Microsoft 365's health monitoring and alerting capabilities, enabling organizations to proactively manage service health and performance. It provides 24/7 service monitoring of critical Microsoft 365 services, including Exchange Online, Microsoft Entra ID, OneDrive for Business, Skype for Business, and Microsoft Teams.

Administrators get instant notifications when service outages, performance degradation, or other critical issues occur. Alerts provide detailed information about the problem, including affected services or components, the number of impacted users, the current status of the issue, and start and end times.

Unlike the native Microsoft 365 service health dashboard, which may have limited historical data retention, AD360 can provide access to historical service health data, enabling trend analysis and proactive problem management. In addition to overall service health, it can monitor the health and performance of specific endpoints accessing Microsoft 365 services. This includes tracking metrics such as response times and request status codes. This granular visibility helps to identify potential bottlenecks or performance issues affecting specific users or devices.

AD360 also allows admins to create their own customizable monitoring profiles and track performance using response times and request statuses to ensure the efficient running of Microsoft 365.

AD360 also aids in preventing data loss through DLP monitoring by analyzing email flow, detecting policy violations, and issuing alerts on sensitive information.

Part 3: Conclusion: Augmenting Microsoft 365 with ManageEngine AD360

While Microsoft 365 provides a robust suite of tools for communication and collaboration, its native management capabilities have certain limitations. These limitations can lead to increased administrative overhead, security vulnerabilities, reduced productivity, and potential compliance issues. AD360 effectively addresses these limitations by providing a comprehensive approach that augments and extends the functionality of the native Microsoft 365 admin center.

AD360 offers enhanced reporting and analytics, streamlined user and license management, advanced security auditing and alerting, and enhanced spam and malware detection. By addressing these critical gaps, AD360 empowers organizations to optimize their Microsoft 365 environments, improve security, and streamline administrative workflows.

ManageEngine
M365 Manager Plus

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus
Exchange Reporter Plus | RecoveryManager Plus

About M365 Manager Plus

ManageEngine M365 Manager Plus is an one-stop solution for Microsoft 365 management, reporting, auditing and monitoring that helps simplify Microsoft 365 governance, administration, and security. M365 Manager Plus enables admins to gain visibility into various Microsoft 365 components and display key insights through more than 700 out-of-the-box reports. It eliminates the need for writing complex PowerShell scripts and reduces costs associated with administering Microsoft 365.

For more information about M365 Manager Plus, visit www.m365managerplus.com.

 **Get Quote**

 **Download**