



Auditing and Reporting in Office 365

Published: June 27, 2016

Introduction

Microsoft Office 365 includes several auditing and reporting features that customers can use to track user and administrative activity within their Office 365 tenant, such as changes made to their Exchange Online and SharePoint Online tenant configuration settings, and changes made by users to documents and other items. Customers can use the audit information and reports available in Office 365 to more effectively manage the user experience, mitigate risk, and fulfill compliance obligations.

This document describes the various auditing and reporting features available in Office 365 and Microsoft Azure Active Directory (Azure AD). This document also provides an overview of internal logging that is available to authorized Microsoft engineers for detection, analysis, troubleshooting, and providing Office 365 services.

Office 365 Security & Compliance Center

The [Office 365 Security & Compliance Center](#) is a one-stop portal for protecting your data in Office 365, and it includes many auditing and reporting features. It is an evolution of the Office 365 Compliance Center. The Security & Compliance Center is designed for organizations that have data protection or compliance needs, or that want to audit user and administrator activity. You can use the Security & Compliance Center to manage compliance for all of your organization's Office 365 data. You can access the Security & Compliance Center at <http://protection.office.com> using your Office 365 admin account.

The Security & Compliance Center includes navigation panes that provide you with access to several features:

- **Permissions** Enables you to [assign permissions](#) such as Compliance Administrator, eDiscovery Manager, and others to people in your organization so that they can perform tasks in the Security & Compliance Center. You can assign permissions for most features in the Security & Compliance Center, but other permissions must be configured using the Exchange admin center and SharePoint admin center.
- **Security policies** Enables you to create and apply device management policies using [Office 365 Mobile Device Management](#) and to set up [Data Loss Prevention](#) (DLP) policies for your organization.
- **Data management** Enables you to [import email or SharePoint data from other systems into Office 365](#), [configure archive mailboxes](#), and set [retention policies](#) for email and other content within your organization.
- **Search & investigation** Provides [content search](#), [audit log](#) and [eDiscovery case management](#) tools to quickly drill into activity across Exchange Online mailboxes, groups and public folders, SharePoint Online, and OneDrive for Business.
- **Reports** Enables you to quickly access [reports](#) for SharePoint Online, OneDrive for Business, Exchange Online, and Azure AD.
- **Service assurance** Provides information about how Microsoft maintains security, privacy, and compliance with global standards for Office 365, Azure, Microsoft Dynamics CRM Online, Microsoft Intune, and other cloud services. Also includes access to third-party ISO, SOC, and other audit reports, as well as Audited Controls, which provides details about the various controls that have been tested and verified by third-party auditors of Office 365.

Some of the features of the Security & Compliance Center are discussed in the following sections.

Content Search

[Content Search](#) is a new eDiscovery search tool in the Security & Compliance Center that provides improved scaling and performance capabilities over previous eDiscovery search tools. You can use Content Search to search mailboxes, public folders, SharePoint Online sites, and OneDrive for Business locations. Content Search is specifically designed for very large searches. There are no limits on the number of mailboxes and sites that you can search. There are also no limits on the number of searches that can run at the same time. After you run a search, the number of content sources and an estimated number of search results are displayed in the details pane on the search page, where you can preview the results, or export them to a local computer. If your organization has an Office 365 Enterprise E5 subscription, you can also [prepare the results](#) for analysis using the powerful analytics features of [Office 365 Advanced eDiscovery](#).

Audit Log Search

In addition to tracking changes in their Office 365 organization, customers can also view audit reports and export audit logs. Once auditing is enabled for an Office 365 tenant, user and administrative activity for that tenant is recorded in event logs and made searchable. For example, you can use mailbox audit logging to track actions performed on a mailbox by users other than the mailbox owner. Further, compliance officers can use the search and filter capabilities to see if a user has viewed or downloaded a specific document, or if an administrator has performed user management activities or made changes to the tenant configuration in the past 90 days. Search results can contain valuable forensic information about specific activities that were conducted by a user or an administrator. See [Audited activities in Office 365](#) for a description of the user and administrative activities that are logged in Office 365.

Events from SharePoint Online and OneDrive for Business are displayed in the log within 15 minutes of their occurrence. Events from Exchange Online appear in the audit logs within 12 hours of occurrence. Login events from Azure AD are available within 15 minutes of occurrence, and other directory events from Azure AD are available within 6 hours of occurrence. Events in audit log search results can also be exported for further analysis.¹ The following table details some of the information that is displayed in activity reports.

Property	Description
Date	The date and time of the event
User	The user who performed the action
ClientIP	The IPv4 or IPv6 address of the device that was used when the activity was logged.
CreationTime	The date and time in Coordinated Universal Time (UTC) when the user performed the activity.
EventSource	Identifies that an event occurred. Possible values are SharePoint and ObjectModel.
Id	The ID of the report entry. The ID uniquely identifies the report entry.
Operation	The name of the user or activity. This value corresponds to the value that was selected in the Display results for this user activity.
OrganizationId	The GUID for the organization's Office 365 service where the event occurred.
UserAgent	Information about the user's browser as provided by the browser.
UserId	The user who performed the action (specified in the Operation property) that resulted in the record being logged.
UserType	The type of user that performed the operation. The following values indicate the user type.

¹ A maximum of 50,000 entries can be exported from a single audit log search. To export more entries than this limit, either reduce the date range, or run multiple audit log searches.

Property	Description
	<ul style="list-style-type: none">• 0 Indicates a regular user.• 2 Indicates an administrator in your Office 365 organization.• 3 Indicates a Microsoft datacenter administrator or datacenter system account.
Workload	The Office 365 service in which the activity occurred. Possible values for this property are: <ul style="list-style-type: none">• Exchange Online• SharePoint Online• OneDrive for Business• Azure Active Directory Reports

Table 1 - Office 365 Activity Report details

For detailed steps to search Office 365 audit logs, see [Searching audit logs in the Office 365 Security & Compliance Center](#).

eDiscovery

The eDiscovery feature provides a single place for administrators, compliance officers, and other authorized users to conduct a comprehensive investigation into Office 365 user activity. Security officers with the appropriate permissions can perform searches and place holds on content. The search results are the same results you get from a Content Search, except that an eDiscovery case is created for any holds that are applied. The results from eDiscovery searches are encrypted for security, and the exported data can be analyzed using [Advanced eDiscovery](#).

Reports

The Reports feature provides a variety of audit reports for Azure AD, Exchange Online, device management, supervisory review, and DLP. These are different and separate from the Office 365 Activity Reports.

Azure Active Directory Reports

Office 365 uses Azure AD for authentication and identity management. Office 365 administrators can use the reports generated by Azure to look for unusual activity and unauthorized access to their data. You can use the access and usage reports in Azure AD to gain visibility into the integrity and security of your organization's directory. With this information, an administrator can better determine where possible security risks may be so that they can adequately plan to mitigate those risks.

Azure AD reports can be exported to Microsoft Excel and correlated with other data from Office 365, such as the results of an audit log search, to provide insight into access, authentication, and application-level activities. Advanced anomaly and resource usage reports are available when Azure AD Premium is enabled. These advanced reports help to improve an organization's security posture and help organizations respond to potential threats by leveraging analytics about device access and application usage. For more information, see the [Azure Active Directory Reporting Guide](#).

Exchange Online Audit Reports

Exchange Online audit reports include details on mailbox access and changes made by administrators to an organization's Exchange Online tenant. Once mailbox auditing is enabled², you can use the tasks in the following table to run reports and export Exchange Online audit logs.

Task	Description
Run a non-owner mailbox access report	Displays the list of mailboxes that have been accessed by someone other than the owner of the mailbox. The report contains information about who accessed the mailbox, the actions they took in the mailbox, and whether or not the actions were successful.
Export mailbox audit logs	Mailbox audit logs contain information on access and actions in a mailbox taken by a user other than the mailbox owner. Administrators can specify mailboxes along with a date range to generate reports. The logs are exported in XML, attached to a message and sent to specific users as determined by the administrator.
Run an administrator role group report	The administrator role group is used to assign administrative privileges to users. These privileges allow users to perform administrative tasks such as reset passwords, create or modify mailboxes, and assign admin privileges to other users. The admin role group report shows changes to role groups, including the addition or removal of members.
View the admin audit log	The admin audit log report lists all create, update and delete functions performed by administrators in Exchange Online. Log entries provide information on which cmdlet was run, what parameters were used, who ran the cmdlet, and what objects were affected.
Mailbox content search and hold	Provides details of any changes to In-Place eDiscovery or In-Place Hold settings on mailboxes.
Export the admin audit log	The admin audit log records specific administrative actions such as create, update and delete in Exchange Online. The results from the log are exported to XML and administrators can choose to send this log to a set of users.
Run a per-mailbox litigation hold report	Provides details of any changes to litigation hold settings on mailboxes.
View and export the external admin audit log	Contains details of actions performed by external administrators. The entries provide information on which cmdlet was run, what parameters were used, and any actions that create, modify or delete objects in Exchange Online.

Table 2 - Mailbox auditing tasks for Exchange Online

Device Compliance Reports

You can manage and secure mobile devices when they're connected to your Office 365 organization by using Office 365 Mobile Device Management (MDM). Mobile devices like smartphones and tablets that are used to access work email, calendar, contacts, and documents play a big part in making sure that employees are able to work anytime, and from anywhere. As a result, it's critical that you protect your organization's information. You can use Office 365 MDM to set device security policies and access rules, and to wipe mobile devices if they're lost or stolen.

MDM compliance reports provide an overview of policies that have been set up by an organization to secure mobile devices that are accessing Office 365 data. The report allows filtering of devices by compliance status, reported violations, blocked devices, and how many devices were wiped as a result of security policies.

For more information, see [Overview of Mobile Device Management for Office 365](#).

² You must [enable mailbox audit logging](#) for each mailbox so that audited events are saved in the audit log for that mailbox. If mailbox audit logging isn't enabled for a mailbox, events for that mailbox won't be saved in the audit log and won't appear in mailbox audit reports. For more information, see [enable mailbox auditing](#).

Data Loss Prevention

DLP policies help manage the security and flow of information in an organization. You can set up policies to block access to content, encrypt data, or notify users of policy and policy violations using in-application DLP Policy Tips. DLP reports provide insight into the number of policy and rule matches, overrides, and false positives.

You can use the Office 365 admin center to view information about the number of messages that are detected by your DLP policies in either graphical chart or table format. Specifically, DLP policy matches for sent and received mail, and DLP rule matches for sent and received mail. You can also view the number of matches, overrides, and false positives for each policy within the past 24 hours using the Exchange admin center. However, this data is not available as a chart. If you download a report for use in Excel, you can view even more detail, such as who sent which message, on what day, and what policy matches were triggered. For more information, see [View reports about DLP policy detections](#).

Service Assurance

Many of our customers in regulated industries are subject to extensive compliance requirements. To perform their own risk assessments, customers often need in-depth information about how Office 365 maintains the security and privacy of their data. Microsoft is committed to the security and privacy of customer data in its cloud services and to earning customer trust by providing a transparent view of its operations, and easy access to independent compliance reports and assessments.

Service Assurance provides transparency of operations and information about how Microsoft maintains the security, privacy, and compliance of customer data in Office 365. It includes third-party audit reports along with a library of white papers, FAQs, and other materials on Office 365 topics such as data encryption, data resiliency, security incident management and more. Customers can use this information to perform their own regulatory risk assessments. Compliance officers can assign the “Service Assurance User” role to give users access to Service Assurance. The tenant administrator can also provide external users, such as independent auditors, with access to information in the Service Assurance dashboard through the [Microsoft Cloud Service Trust Portal](#) (STP). For details on how to access the STP, visit [Get started with the Service Trust Portal for Office 365 for business, Azure, and Dynamics CRM Online subscriptions](#).

Search Unified Audit Log

As described above, the Audit Log Search feature in the Security & Compliance Center can be used to search the unified audit log. Office 365 also provides the ability to search this log using remote PowerShell. Specifically, the [Search-UnifiedAuditLog](#) cmdlet in Exchange Online PowerShell can be used to search the unified audit log of events relating to user operations from Exchange Online, SharePoint Online, OneDrive for Business, and Azure AD. You can search for all events in a specified date range, or you can filter the results based on specific criteria, such as a specific action, the user who performed the action, or the target object. Administrators can use up to 3 simultaneously running Exchange Online PowerShell sessions to split up large date range searches.

Auditing in Yammer Enterprise

Yammer Enterprise provides administrators with the ability to export user activity data from their Yammer network(s) via the [Yammer Data Export API](#), or manually via the Yammer network admin page.

The ability to export logs is restricted to Network Administrators in Yammer.³ The following data can be exported:

Filename	Description
Users.csv	All new, pending, and suspended users in the network
Messages.csv	All messages in the network
Files.csv (metadata)	Metadata such as filename, file API URL, uploader ID, uploaded at, etc.
Files.csv (Original files)	Zip file of the original files that were uploaded by users into Yammer
Topics.csv	Topics created on the network
Pages.csv	Pages (notes) created by users in the network
Admins.csv	All verified administrators on the network
Networks.csv	All Yammer external networks

Table 3 - Yammer network data files available for export by customers

Yammer Enterprise data is also available through the Office 365 Activity Reports. In addition, Yammer is actively working on exposing additional logging via the Office 365 Management Activity API, and on the ability to reason over data using Power BI. See the [Office Roadmap](#) for more information on these features.

Office 365 Management Activity API

Microsoft provides reporting services that enable administrators to obtain aggregated transactional information about their Office 365 tenant. The Office 365 Management Activity API uses an industry-standard RESTful design and OAuth v2 for authentication, which makes it easy to start experimenting with retrieving data and ingesting it into visualization tools and applications. The API provides a data feed that includes information about user, administrator, operations, and security activity in Office 365. The data can be kept for regulatory purposes, or combined with log data procured from an on-premises infrastructure or other sources to build a monitoring solution for operations, security, and compliance across the enterprise.

The Management Activity API currently provides a comprehensive view of over 150 transaction types from SharePoint Online, OneDrive for Business, Exchange Online and Azure AD. The API provides a consistent audit schema with over 10 fields that are in common across all the services. This allows organizations to make easy connections between events, and it enables new ways to reason over the data. Dozens of Independent Software Vendors (ISVs) have partnered with Microsoft and built solutions based on the API. Some solutions are focused solely on Office 365 data, while others provide the ability to ingest data from multiple cloud providers and on-premises systems to create a unified view of all operations, security, and compliance-related activity. For more information, see the [Office 365 Management Activity API reference](#).

Office 365 Reports Dashboard

The Reports dashboard in the Office 365 Admin center preview displays usage activity across Office 365. Office 365 global administrators, or an Exchange Online, SharePoint Online, or Skype for Business administrator, can get granular insight into the usage of that service. Reports can provide insights such as the number of users consuming a particular Office 365 service, the number of users that have

³ All Office 365 global administrators are Yammer Network Administrators.

activated Office Professional Plus, and how much mail is flowing through the organization. Reports are available for the last 7, 30, 90, and 180 days.

The following reports are available:

- [Email activity reports](#)
- [Microsoft Office activation reports](#)
- [SharePoint Online Site usage reports](#)
- [OneDrive for Business usage reports](#)
- [Yammer Enterprise activity reports](#)
- [Skype for Business activity report](#)
- [Skype for Business Peer-to-Peer activity report](#)
- [Skype for Business Conference Organizer report](#)
- [Skype for Business Conference Participant activity report](#)

For more information, see [Activity Reports in the Office 365 Admin Center Preview](#).

Mailbox Migrations

With an Exchange-based hybrid deployment, customers can choose to either move on-premises Exchange mailboxes to an Exchange Online organization or move Exchange Online mailboxes to an Exchange on-premises organization. Migration batches are used when moving mailboxes between on-premises and Exchange Online organizations. Customers can review statistics and other information about mailbox migrations using the following cmdlets:

- [Get-MoveRequestStatistics](#) Provides default statistics for a user mailbox, which includes the status, mailbox size, archive mailbox size and percentage complete.
- [Get-Mailbox](#) Provides a summary list of mailbox objects and attributes in the organization.
- [Get-Recipient](#) Provides a list of existing mail-enabled objects such as mailboxes, mail users, contacts and distribution groups.
- [Get-MoveRequest](#) Provides a detailed status of an ongoing mailbox migration.
- [Get-MigrationUser](#) Provides information about the mailbox move and migration users.
- [Get-MigrationBatch](#) Provides information on the status of current migration batch.
- [Get-MigrationUserStatistics](#) Provides detailed information about the migration status for a specific user.
- [Get-MailboxStatistics](#) Provides information about mailboxes, such as size, the number of messages, and the last accessed time.

For more information on additional cmdlets, see [Move and Migration cmdlets in Exchange Online](#).

Internal Logging for Office 365 Engineering

In addition to the events and log data described above that is available for customers, there is also an internal log data collection system that is available to Office 365 engineers. Many different types of log data are uploaded from Office 365 servers to an internal, big data computing service called Cosmos. Each service team uploads audit logs from their respective servers into the Cosmos database for aggregation and analysis. This data transfer occurs over a FIPS 140-2-validated TLS connection on

specifically approved ports and protocols using a proprietary automation tool called the Office Data Loader (ODL).

Service teams use Cosmos as a centralized repository to conduct an analysis of application usage, to measure system and operational performance, and to look for abnormalities and patterns that may indicate problems or security issues. Each service team uploads a baseline of logs into Cosmos, depending on what they are looking to analyze, that often include:

- Event logs
- AppLocker logs
- Performance data
- System Center data
- Call detail records
- Quality of experience data
- IIS Web Server logs
- SQL Server logs
- Syslog data
- Security audit logs

Prior to uploading data into Cosmos, the ODL application uses a scrubbing service to obfuscate any fields that contain customer data, such as tenant information and end-user identifiable information, and replace those fields with a hash value. The anonymized and hashed logs are rewritten and then uploaded into Cosmos. Service teams run scoped queries against their data in Cosmos for correlation, alerting, and reporting. The period of audit log data retention in Cosmos is determined by the service teams; most audit log data is retained for 90 days or longer to support security incident investigations and to meet regulatory retention requirements.

Access to Office 365 data stored in Cosmos is restricted to authorized personnel. Microsoft restricts the management of audit functionality to the limited subset of service team members that are responsible for audit functionality. These team members do not have the ability to modify or delete data from Cosmos, and all changes to logging mechanisms for Cosmos are recorded and audited.

Each service team accesses its log data for analysis by authorizing certain applications to conduct specific analysis. For example, the Office 365 Security team uses data from Cosmos through a proprietary event log parser to correlate, alert, and generate actionable reports on possible suspicious activity in the Office 365 production environment. The reports from this data are used to correct vulnerabilities, and to improve the overall performance of the service. If a specific alert or report requires further investigation, service personnel can request that data be imported back into the Office 365 service. Since the specific log being imported from Cosmos is in encrypted and service personnel do not have access to decryption keys, the target log is programmatically passed through a decryption service that returns scoped results to the authorized service personnel. Any vulnerabilities found from this exercise are reported and escalated using Microsoft's standard security incident management channels.

Summary

Office 365 includes several reporting features in the Office 365 Security & Compliance Center, and programmatic methods for retrieving and analyzing log data using remote PowerShell and a Web Services REST API. Customers can use the reporting and auditing features in Office 365 to track changes made to key tenant and service configuration items, to documents, and to other items. Office 365 tenant administrators can use the reports generated in Azure to help look for unusual activity or unauthorized access to their data. Yammer Enterprise provides administrators with the ability to export data from their Yammer network via the Yammer Data Export API. Office 365 Service Assurance provides access to third-party audit and compliance reports, and trust documents that help customers perform their own risk assessment of Office 365.

Finally, log data is uploaded from Office 365 servers to an internal big data computing service called Cosmos. Office 365 service teams upload audit logs from their respective service hosts into Cosmos over a FIPS 140-2-validated TLS connection on specific approved ports and protocols for aggregation and analysis. Analysis of this data is used for correlation, alerting, and reporting, and ultimately to correct vulnerabilities and improve the overall performance of Office 365.