6 ways to get more out of your SharePoint audit logs

ManageEngine
SharePoint Manager Plus

Table Of Contents

The dread of auditing SharePoint

Microsoft SharePoint, as a content management and collaboration tool, has changed the way people collaborate and run their businesses.

Organizations worldwide have leveraged SharePoint to house sensitive business data and build custom web applications in the pursuit of seamless collaboration among employees.

According to Gartner, end-user spending for the information security market is estimated to reach $170 billion by the end of 2022.

However, as organizations expand and data grows, with this growth comes a maelstrom of uncertainties around who has access to what.

Not having proper provisions to audit SharePoint environments can result in accidental policy violations going unnoticed. Besides causing compliance nightmares down the line, they can also snowball into a cascade of failures that can affect overall employee efficiency or lead to security incidents.

In this e-book, we will discuss in detail the benefits of auditing your SharePoint infrastructure, the challenges in using just the native tools, and how SharePoint Manager Plus—a web-based SharePoint management, auditing, and reporting solution—can help you simplify SharePoint auditing.

Meeting legal obligations and regulatory compliance

Regardless of an organization's size or industry vertical, it is mandatory for the organization to abide by the IT regulatory compliance mandates it falls under.

SharePoint helps organizations facilitate seamless collaboration among their employees. At the same time, organizations must ensure that they stay compliant. However, as organizations expand, the number of objects grows exponentially, increasing the chances of crucial change events on an object slipping under the radar.

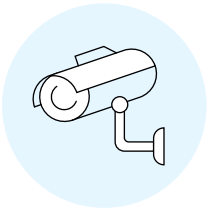
This is why the ability to spot and follow up on security infractions can help organizations avoid hefty fines levied for accidental compliance violations. Auditing your SharePoint environment diligently with the help of audit logs can help ensure this.

Aside from this, employees are less likely to ignore security best practices when they know that their actions are audited closely.

Safeguarding intellectual property and improving business processes

Managing an enterprise-level SharePoint environment is a chore. As the data and users grow, it becomes quite easy to lose track of who has access to what. Having a good understanding on the SharePoint files and folders in any site collection helps in deciding who should and should not have permission to access it.

Apart from a security standpoint, understanding the content housed by SharePoint can help optimize business processes. With the help of the information available from auditing SharePoint, organizations can understand what content is widely used by their employees; what content is not being used and why; and distribute future investments based on the findings.



Quickly spotting security loopholes and taking remedial measures

Whenever an undesired change is made on an important object— say a file containing human resources data, it must be brought to the administrator's attention as soon as possible.

Say the file is deleted either accidentally or by a disgruntled employee. Using the audit logs, the administrator can figure out who deleted the file and retrieve it quickly in addition to implementing proactive countermeasures to ensure that this event does not happen again.

The limitations of SharePoint auditing using native tools

SharePoint has a built-in audit feature to track user activity on content types like lists and libraries within your site collection to give you a good oversight on what is happening in your SharePoint environment. However, using just the native tools can often make SharePoint auditing difficult.

The following is the list of events you can track with the help of audit logs.

- Opened and downloaded documents, viewed items in lists, or viewed item properties (this event is not available for SharePoint in Microsoft 365 sites)
- Edited items
- Checked-out and checked-in items
- Items that have been moved and copied to another location in the site collection
- Deleted and restored items
- Changes to content types and columns
- Search queries
- Changes to user accounts and permissions
- Changed audit settings and deleted audit log events
- Workflow events
- Custom events

The reports generated on the above events are not categorized by objects, which makes it difficult to analyze. Also, since the change events are recorded by object ID, it's a major challenge to interpret the information and come to any logical conclusion.

Also, since these reports can only be exported in Excel format, you might either have to sift through thousands of lines of raw data manually or use pivot tables in Excel to sort, filter, and analyze an event, making the process highly inefficient and time-consuming. Further, if you have huge amounts of audit data, SharePoint would allow exporting them in multiple excel files, which makes it even more difficult to arrive at any logical conclusion about the event under audit.

SharePoint audit logs do not provide adequate information on a change event. They fail to provide information on the values before and after a modification. For instance, say an unwanted change event occurred, merely being aware of it wouldn't help ensure that this change does not occur in the future. You need to be able to know what the permissions were before and after the change to assess the situation accurately and plug any potential security loopholes.

How SharePoint Manager Plus simplifies SharePoint auditing

ManageEngine SharePoint Manager Plus helps simplify SharePoint auditing by overcoming the limitations discussed above and more. Using SharePoint Manager Plus, you can generate audit reports for both on-premises and Office 365 SharePoint environments via a central web console.

Effortless object-specific auditing

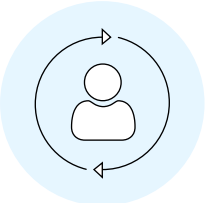
You can audit events related to any objects such as libraries, lists, SharePoint users, or groups with the help of pre-categorized audit reports. Unlike in the native build, the raw data is converted into useful information before the report is generated. Object IDs are converted into names that help reading the audit report without any difficulty.

Exporting audit reports in multiple formats

Audit reports generated can be exported in multiple formats, including XLS, CSV, PDF, and HTML. This makes it easier to analyze your environment.

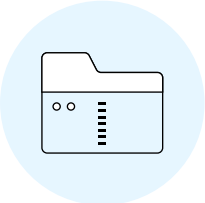
Enabling auditing efficiently

In the native build, you would have to enable auditing for each of your site collections independently. This is both time-consuming and inefficient. However, using SharePoint Manager Plus, you can enable auditing for all site collections in your environment together in just a few clicks. You can also choose the different audit events that need to be tracked for site collections.



Before and after values of every change event

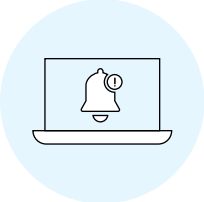
You can track the new and old values of a change event to stay aware of what the permissions or titles were previously set and modified. This expedites forensic analysis, thereby reduces the time between a security mishap and the corresponding remedial measure.



Audit logs archiving

Audit logs are stored in the SharePoint content database. Since these audit logs can grow enormously over time, the sheer volume of these audit logs, if left unchecked, could inflate the SharePoint content database and slow down SharePoint response time and operations. One workaround would be to download these audit logs as files and store them in the IT administrator's computer. However, this might raise security concerns.

A widely accepted security best practice is to transfer these audit logs quickly — if possible, in real-time — to a secure log repository like SharePoint Manager Plus to safeguard the integrity of the audit logs and offset the risk of any compliance violations. Using SharePoint Manager Plus audit logs can be archived and restored as needed. This helps you meet compliance regulatory requirements and look up audit logs easily when necessary.



Schedule alerts and audit reports

SharePoint Manager Plus lets administrators define alert profiles for different SharePoint change events. When a change event matching the alert profile occurs, the administrator can receive a real-time email notification. This helps administrators to roll back any undesired security change made in the SharePoint environment. Administrators can also schedule audit reports to be emailed to themselves or any user on a daily, weekly, or monthly basis.

ManageEngine
SharePoint Manager Plus

ManageEngine SharePoint Manager Plus is a tool that helps you to manage, audit, report both the on-premises and Office 365 SharePoint environments. It also allows you to monitor, track and analyze all the activities in your SharePoint infrastructure which facilitates informed, timely and accurate decision making and management.

$ Get Quote Download