ManageEngine
ADAudit Plus

Automate compliance reporting

for all major audits, including

SOX, HIPAA, PCI DSS, FISMA, GLBA, and ISO 27001

www.adauditplus.com

Automate compliance reporting for all major audits, including SOX, HIPAA, PCI DSS, FISMA, GLBA, and ISO 27001

Regardless of the compliance requirement that you are trying to fulfill, the current methods for generating reports are inefficient, ineffective, and fail to truly provide information that can ensure network security. Auditors, administrators, and security professionals need solutions that provide them with quality reports in a time frame that captures the correct security information.

One way to solve these major concerns with today's compliance reporting is to use automation to generate reports. Automating report generation can solve not only the concerns around inefficiency and ineffectiveness, but can also ensure current security configurations are provided and reports are secured. More importantly, automating report generation ensures your security compliance reports are accurate and available when you need them.

Inefficiency of current reporting methods

Nearly all audits for major compliance regulations, like SOX, HIPAA, PCI DSS, FISMA, GLBA, and ISO 27001, are performed oncee a year. This means that auditors must request reports for each compliance regulation at the time of the audit. In some cases, reports from one audit can be used for another audit. This does provide added value in making at least a portion of the audit more efficient. However, the current method for obtaining reports is not efficient for anyone involved in the process.

Administrators must generate reports

For me personally, performing audits over the past 15 years has proven to be a frustrating process for everyone involved. In general, auditors, administrators, and security professionals do not look forward to any audit, due to the time required to gather reports, analyze them, and write up the results. Just looking at the first two steps in the audit process exposes major concerns about efficiency.

1. Auditors must request reports from administrators.
2. Administrators are required to take the time to generate auditor reports.
3. Often, one report doesn't correctly provide the information needed by the auditor, so administrators need to generate more reports.
4. There is no standard for report generation, forcing administrators to use different tools and report structures, as well as generate various file types.
5. Without consistent report structures and content, report analysis can take much longer than expected.

All of these factors result in auditors and administrators spending a significant amount of time on report generation and analysis. If these concepts could somehow be altered to ensure reports are generated the same way each time and are always available to the auditor, the overall audit process could be made more efficient.

Auditors must wait for reports

Since auditors do not have the privileges required to generate security-based reports, they must follow procedures to request reports. Unfortunately most auditors are not intimately familiar with the operating system or application they need the report from, so they are left to describe the report content they are looking for.

Administrators, on the other hand, are busy employees. They do not have extra bandwidth to work full time with the auditor to ensure that the reports produced are 100 percent accurate. This leaves administrators to decide which tools to use and what format they should use to produce the reports. During this time, the auditor must wait for the administrator to send them the report.

In many cases, the report that the administrator produces does not meet the auditors' detailed requirements, so the entire process must be repeated, from describing what is needed to guessing which tool/format to use for each report.

Ideally, if everyone involved in the audit could determine which format is most efficient for analysis and select a tool to produce the correct content and format, the entire process could be automated. If the reporting process was automated, auditors could have reports waiting for them at all times. The reports would also include the most recent security settings, not to mention historical reports that indicate any changes over time.

Ineffectiveness of current reporting methods

Most of today's compliance audits are done as point-in-time audits. This means that once a year (at best) reports are generated on the desired security settings and configurations. Then the auditor analyzes these reports to determine if the organization's security meets certain compliance requirements. If the current settings do not meet compliance requirements, the final report will indicate that the administrator needs to alter their settings.

The issue with this concept is that the only data the auditor is only analyzing is a split second in time. The week, month, or year before the report was

generated isn't included on reports; there's no indication of what the security setting has been, only what it is at the time of the report. Unfortunately this is not the only issue; there are other potential scenarios which make this type of audit process invalid:

1. What if the administrator changes the security setting seconds before running the report, only to change it back after running the report?
2. What if the security setting was incorrectly configured for a week, leaving the network exposed, but is correct at the time of running the report?
3. What if the administrator alters the security setting per the final report from the auditor, only to change it a week after the auditor moves on to the next project?

The goal of any compliance regulation and audit is to verify that the proper security standards are in place. However, just looking at a single second during an entire year only verifies that one second, not the other 364 days, 23 hours, and 59 minutes.

In order for compliance to truly be upheld, and security to be in place, auditors must be able to constantly receive reports proving that the security settings are not changing. If auditors can receive constant reports and alerts for all changes to security settings, this is considered true continuous auditing. True continuous auditing is the best form of security to ensure that a network is protected.

(Refer to this white paper for additional information on true continuous auditing.)

Auto-generating reports

Instead of performing audits that are inefficient and ineffective, let's consider another option: automation. Using automation to generate reports solves the major issues listed above, with a few added benefits:

1. Reports will always follow a standard format and structure from audit to audit.
2. Reports can be generated once a day, week, month, etc.
3. Auditors will not need to ask administrators to generate reports.
4. Administrators will not need to take time and iterations to generate reports.
5. Auditors will be able to analyze reports over time, instead of just at a single point in time.
6. Auditors can easily view and analyze security changes.
7. All security setting and configuration reports can be customized for automation.

Reports per compliance regulation

Each compliance regulation has a unique set of requirements; therefore, each regulation has its own set of required reports. Trying to decrypt these reports can be time-consuming, confusing, and frustrating. Ideally, once an organization has determined what reports it needs for each of the compliance requirements, they can just duplicate the reports for each cycle of the audit. This is exactly what the ManageEngine suite of tools has done for each of the major compliance regulations.

Log360 (which includes EventLog Analyzer and ADAudit Plus) provides reports for each compliance regulation, giving you a quick and easy way to automatically produce compliance reports.

As many administrators have seen, there are some special reports that are required based on their company's needs, their operating systems and applications, or perhaps even the external auditor's interpretation of the regulations. In order to meet these requirements, custom reports might be

needed. It is essential that these custom reports be easy to design and implement, as well as automate. ManageEngine's products are built to include custom reports that are very simple to create.

Since each organization has different needs with regard to generating reports for audits and analysis, all reports should have options for scheduling. There should be a good balance between reports generated and reports being reviewed and analyzed. Too many reports can overwhelm the auditing staff, while too few reports won't give auditors enough information for good analysis. The ManageEngine product suite provides report-level scheduling for automating report generation.

By default, compliance reports contain security-related information. If the wrong person can see the contents of compliance reports, it could result in a breach of some kind. Therefore it is imperative that these reports be secured. Ideally, report automation will store the reports in a secure folder which is only accessible by approved IT, security, and audit staff. Again, ManageEngine allows you to store reports in a folder of your choosing, which can of course be locked down with security permissions.
(Note: Log360 provides file and folder-level permission monitoring, generating an alert if any of the permissions change on a file or folder.)

Automate common reports

Each compliance regulation has a different set of requirements for Windows security reports. That being said, there are some reports that are common across multiple compliance regulations. Log360 provides reports which are separated by the compliance regulation that you are focusing on. For instance, Figure 1 illustrates reports for SOX compliance.

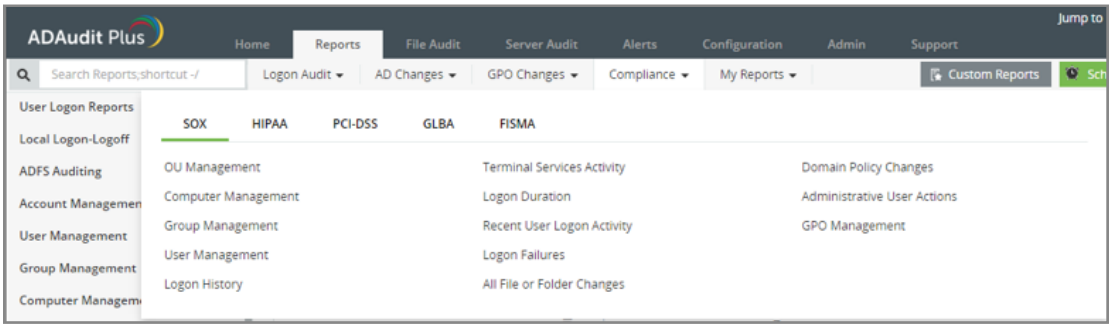

Figure 1. Log360 provides detailed reports that cover all key compliance regulations.

As you can see in Figure 1, Log360 supports all of the key compliance regulations.

Automate custom reports

In many cases, a compliance regulation goes beyond the basic operating system installation and requires organizations to report on customized configurations. These requirements force administrators to produce reports that aren't available in any kind of reporting solution, as the objects being reported on are unique to each organization. Tools such as Log360 enable administrators to create custom reports, allowing them to meet these specific areas in compliance regulations. Figures 2 and 3 illustrate custom reports.

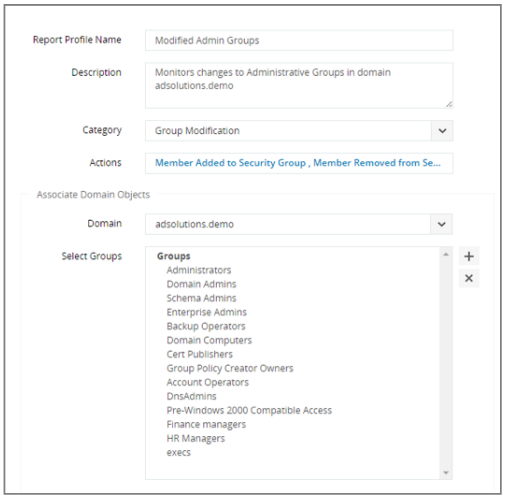

Figure 2. A custom report using a built-in report as a foundation in Log360.

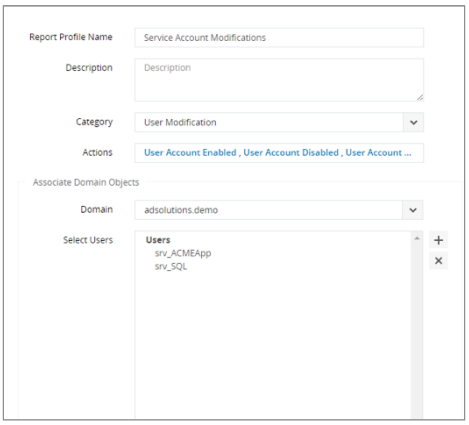

Figure 3. A custom report focusing on any changes to service accounts.

With Log360, any built-in report can be customized; administrators can also develop many custom reports using complex and detailed security requirements.

Automate and schedule report generation

As you can see, Log360's built-in and custom reporting capabilities are powerful. Any and all reports that are available in Log360 can also be automated and scheduled. This provides a thorough view of all the changes for the compliance areas and settings that you need to report on.

Creating automations for each and every report is easy using Log360. Once you've opened a report in ADAudit Plus, simply select the "Add to" button and select "Schedule this report"

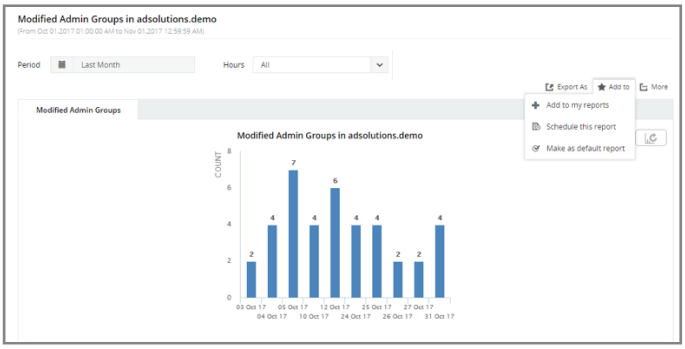

Figure 4. Scheduling a report in Log360.

This will send you directly to the report scheduler, shown in Figure 5.

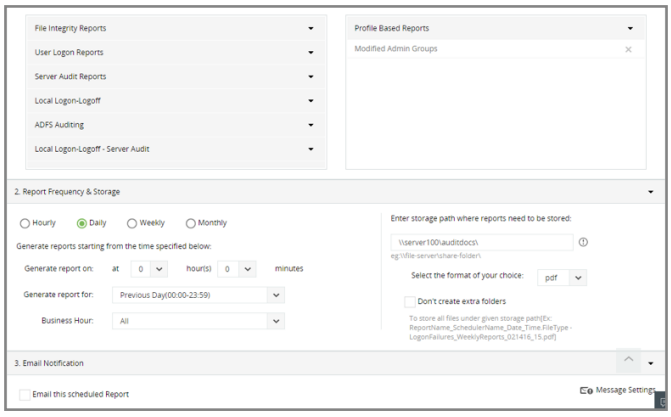

Figure 5. Report Scheduler in ADAudit Plus.

Now you simply select how often you'd like to generate the report (frequency), along with the details shown in Figure 5. You can also ensure that an email is sent every time this report is automatically generated.

Once you have all of your compliance reports scheduled to automatically generate, you'll have time to do your other administrative tasks.

Summary

Compliance can be a tedious task. There are many compliance regulations out there, each requiring separate reports. Ideally, these reports would be automatically generated and emailed to the appropriate people in your organization when they're completed. While Microsoft does not provide an efficient and effective solution for automatic report generation, ADAudit Plus from ManageEngine is the ideal solution to solve all of your reporting needs.

To see how easy ADAudit Plus is to configure and use, not to mention the power it has, you can download it from here and try it out yourself.

About ADAudit Plus

ADAudit Plus is an IT security and compliance solution designed for Windows-based organizations. It provides in-depth knowledge about changes effected to both the content and configuration of Active Directory and servers. Additionally, it provides thorough access intelligence for desktops and file access in servers (including NetApp filers), enabling you to protect organization data.