ADAudit Plus Review – Active Directory Monitoring Solution

Last updated October 4, 2024 by Rudy Mens
#sponsored

ADAudit Plus is an auditing tool designed to monitor and audit Active Directory (AD) environments. It provides insights into user activities, login attempts, configuration changes, group membership modifications, and much more across your network.

The strength of ADAudit Plus is that it transforms raw event data into actionable reports and alerts. This information allows you to stay on top of changes that occur in your AD environment, such as those related to users, groups, and computers, ensuring no detail goes unnoticed.

In this article, we take a look at the capabilities of ADAudit Plus, how to get started, and talk about some tips to get the most out of it.

Overview of ADAudit Plus

ADAudit Plus is an essential tool for keeping your AD secure and compliant. It helps track changes, manage user logins, and analyze potential threats. The software is equipped with many built-in reports and real-time alerts to give you clear insights and enhanced security.

The software can also flag anomalies like unexpected login times or login attempts on disabled accounts. Furthermore, with its ability to audit account lockouts and password changes, it helps detect unauthorized access while also providing essential data for troubleshooting issues.

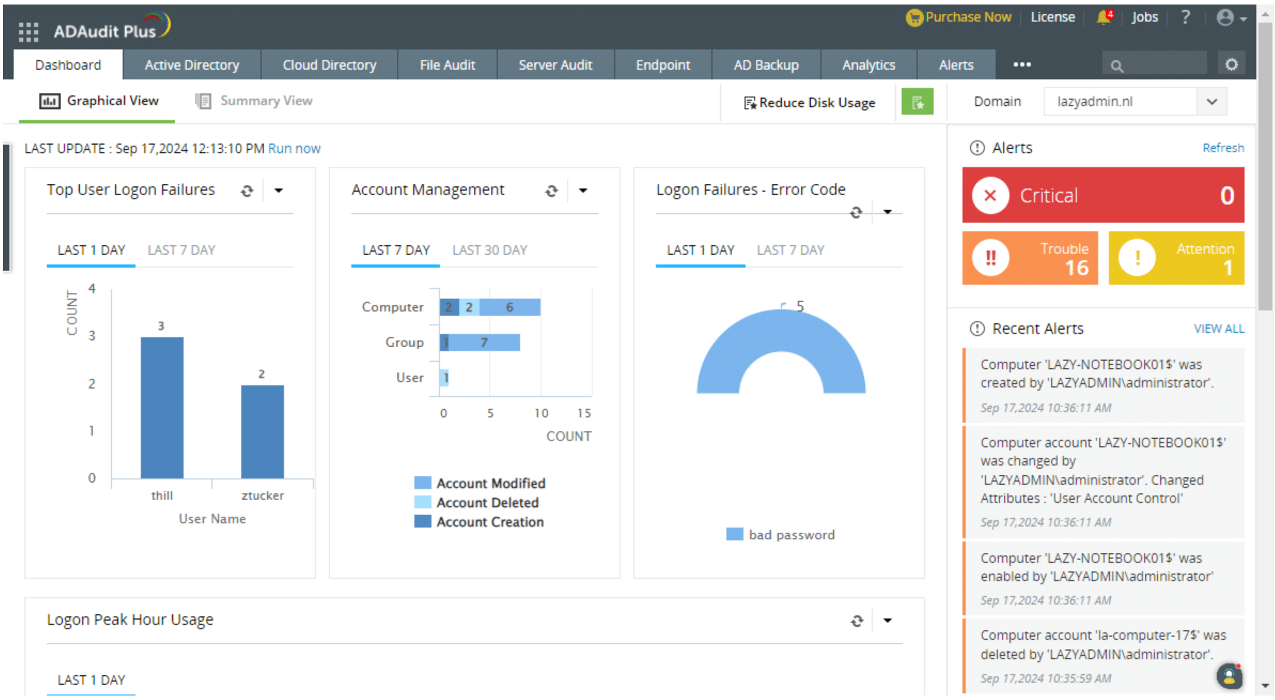
The tool is not limited to monitoring your AD alone. There are several add-ons that you can purchase that allow you to monitor all the vital parts of your IT environment:

- Cloud Directory (like Entra ID)
- File Server monitoring
- NAS Auditing (NetApp, EMC, Synology, Qnap, Azure File Share, Amazon FSx)
- Member Server auditing
- Endpoint Analytics

These capabilities ensure that your infrastructure is not only secure but also compliant with industry standards. This blend of features makes ADAudit Plus a go-to solution for many seeking effective AD audits.

User Interface Overview

ADAudit Plus features a user-friendly interface designed to make navigation straightforward, even for those new to audit systems. The dashboard provides an organized view of key metrics and important alerts at a glance. You can quickly access numerous built-in reports that are customizable to fit specific organizational needs.



Computer 'LAZY-NOTEBOOK01$' was created by 'LAZYADMIN\administrator'.
Sep 17,2024 10:36:11 AM

Computer account 'LAZY-NOTEBOOK01$' was changed by 'LAZYADMIN\administrator'. Changed Attributes : 'User Account Control'
Sep 17,2024 10:36:11 AM

Computer 'LAZY-NOTEBOOK01$' was enabled by 'LAZYADMIN\administrator'
Sep 17,2024 10:36:11 AM

Computer account 'la-computer-17$' was deleted by 'LAZYADMIN\administrator'.
Sep 17,2024 10:35:59 AM

This setup allows you to generate detailed reports on user activity or policy changes with ease. The interface's simplicity aids in reducing the learning curve and ensures that you can effectively manage audits without the complicated processes typical of some auditing software. This makes it a valuable tool for teams focused on maintaining security and compliance.

System Requirements

ADAudit Plus is compatible with Windows Server operating systems. You'll need a minimum of 8GB of RAM and 50GB of disk space, but for optimal performance, you should have double those at least.

For database management, ADAudit Plus works with PostgreSQL (bundled). It's however possible to change this to MS SQL after the initial installation. For large environments with high event volumes, it's recommended to use a dedicated server.

The application is fully web-based and can be accessed from any domain computer if you have the correct credentials. I do recommend enabling and using the HTTPS port for the application. It's also a good idea to configure the single sign-on if you want to use the application with multiple technicians.

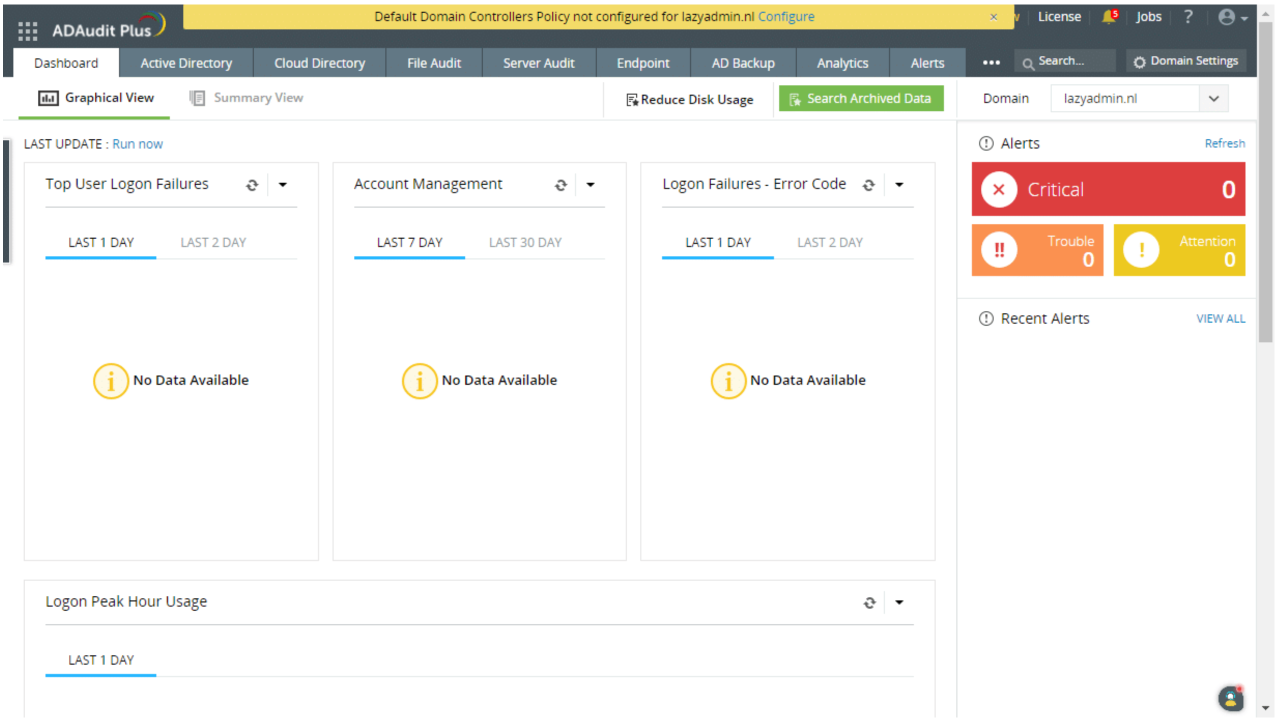
Installation and Configuration

ADAudit Plus offers a straightforward setup process and flexible configuration options. The software's user-friendly interface guides you through initial installation and policy setup to quickly get your AD auditing up and running.

Initial Setup Process

To begin, download the ADAudit Plus installer from ManageEngine's website. Run the executable and follow the installation wizard prompts. Select your preferred installation directory and choose the standalone setup.

During installation, you'll need to specify the database type — either the built-in PostgreSQL or an existing SQL Server instance. The software will then configure the necessary services and open the required ports, typically 8081 for web access.



Default Domain Controllers Policy not configured for lazyadmin.nl Configure

Domain: lazyadmin.nl

LAST UPDATE : Run now

No Data Available

After installation is complete, access the web console using the provided URL. Log in with the default credentials and change them immediately for security. The initial configuration wizard will help you connect to your AD domain and set up basic auditing parameters.

Alert Profiles

Once connected to your domain, ADAudit Plus simplifies the process of enabling necessary audit policies. Navigate to the Configuration section in the web interface to access the Alert Profile settings.

Most of the profiles are enabled by default, which is in most cases too much, to be honest. With too many alerts enabled, you risk getting alert fatigue, such that you might be inclined to simply ignore the alerts. So I recommend going through the alert profiles and disabling everything you don't need.

There are also some alert profiles disabled by default. Some of those, like the **Disabled Users Logon Attempt**, are quite interesting to activate. This one in particular is interesting because we want to know which process is still trying to use the account in question.

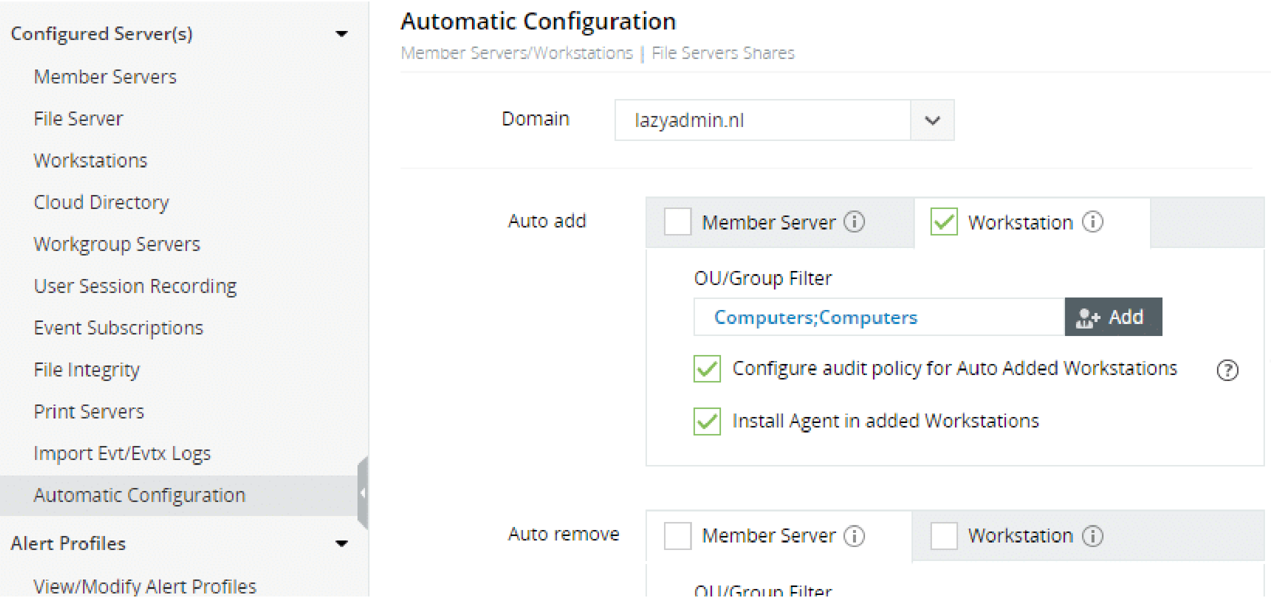
Each alert profile can be fine-tuned by using the filters, allowing you to select specific users, groups, or OUs to monitor. This targeted approach helps manage data volume and focuses on critical assets.

Remember to review and adjust your audit policies periodically to ensure that they align with your evolving security needs and compliance obligations.

Client Agent

The ADAudit Plus client agent is a lightweight software component that extends the tool’s capabilities to individual workstations and member servers. This agent enables detailed auditing of local events that aren’t captured in the central AD logs.

With the client agent, you can monitor local user logons, application usage, and file access on endpoint devices. This granular visibility helps you track user behavior and detect potential security risks at the endpoint level.



Automatic Configuration

Domain: lazyadmin.nl

Auto add: □ Member Server ☑ Workstation

OU/Group Filter: Computers;Computers

☑ Configure audit policy for Auto Added Workstations

☑ Install Agent in added Workstations

Auto remove: □ Member Server □ Workstation

OU/Group Filter

The agent is easy to deploy and manage centrally through the ADAudit Plus console. It has minimal impact on system performance and can be configured to send data in real time or at scheduled intervals to optimize network usage.

Monitoring with ADAudit Plus

With ADAudit Plus, you can take advantage of **real-time monitoring**. This feature enables you to see changes as they happen. Whenever there is an alteration to user accounts, such as logins or modifications of group policies, you receive instant notifications.

This quick response is crucial for maintaining secure IT operations. You also gain insight into password history and login activities, which can help you prevent unauthorized access.

Notifications can be customized to suit specific needs so that you can stay informed about relevant changes without sifting through unnecessary data.

What you should monitor

When using ADAudit Plus, focus on monitoring key areas that impact your AD security and performance. Track user account activities, including creations, deletions, and modifications. Keep an eye on group membership changes, but focus on privileged groups.

Monitoring logon events may seem useful, but it doesn’t really add any value. Instead, only monitor the successful and failed login attempts outside business hours for the normal user accounts. And monitor the first sign-ins and failed sign-ins of service accounts.

When it comes to monitoring general login failures, a single or double login failure. for example, isn’t something to worry about. But when a password is entered 5 times incorrectly, it becomes interesting.

ADAudit Plus allows you to set up custom reports for these critical areas, helping you stay on top of your AD environment’s security posture.

Analyzing Audit Data

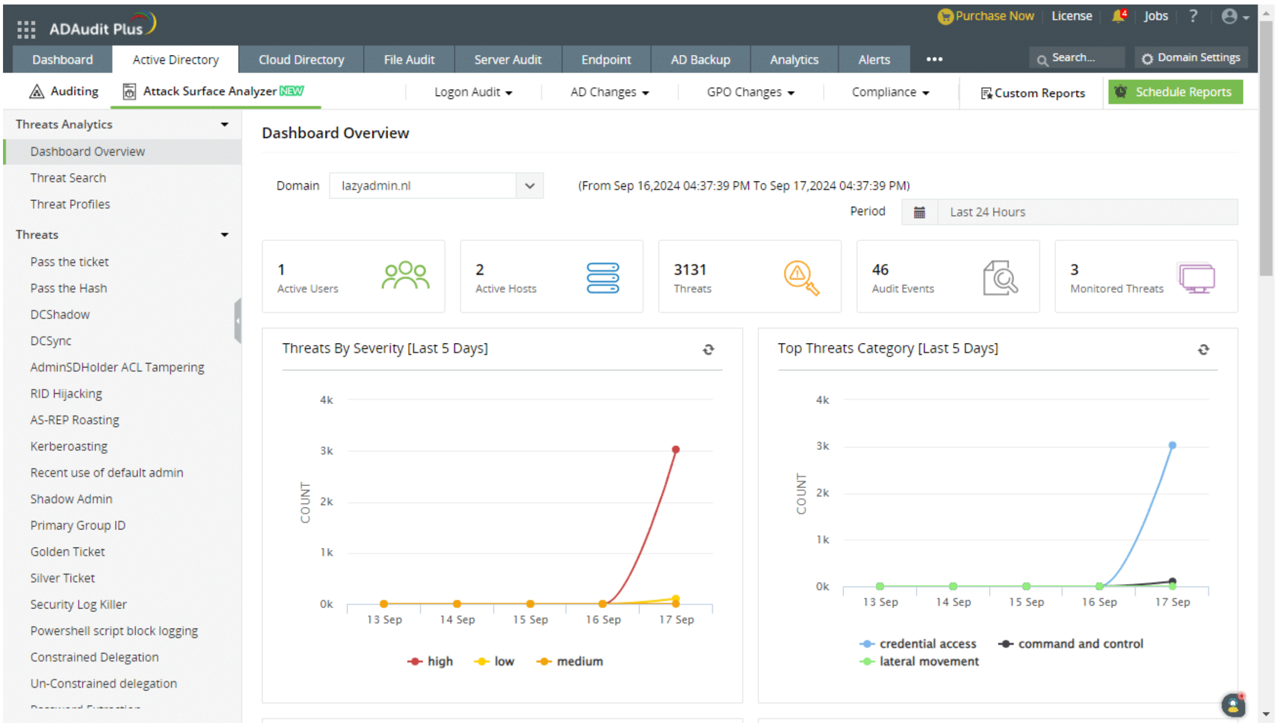
AdAudit Plus gathers a lot of data. To analyze all the data, we can use a wide variety of reports that allow you to track and zoom in on all the different activities. These reports cover pretty much every aspect of your AD environment.

Good to know is that you can customize these reports to fit your specific needs, ensuring that you only see the most relevant information.

The dashboard displays these reports in an easy-to-read format. This readability makes it simple to keep track of ongoing activities within your network. Reports can be exported for further analysis or sharing with your team. This ensures that everyone has access to vital information.

Attack Surface Analyzer

A pretty new feature of ADAudit Plus is the Attack Surface Analyzer. It can detect over 25 different types of attacks. These attacks include stealing passwords, moving through the network without permission, and trying to gain more control than allowed. It can also find risky settings in Azure, like making a virtual machine public, which can lead to attacks.



Using the MITRE ATTACK framework, ADAudit Plus can spot over 15 types of network attacks and 20 types of process attacks. It uses machine learning to detect unusual activities, like when someone uses a special permission for the first time.

Ensuring Security and Compliance

With ADAudit Plus, you can effectively audit changes and manage compliance. These features help you maintain a secure and compliant environment by providing detailed insights and automated alerts.

Change Auditing

Change auditing is essential to track modifications in your AD. ADAudit Plus allows you to monitor user activities, such as logins, password changes, and group membership updates. This continuous surveillance ensures you can detect unauthorized changes quickly and react promptly.

Automatic alerts notify you of unusual activities like mass user account lockouts or configuration changes. By transforming raw data into reports and alerts, ADAudit Plus gives you a clear view of your network’s health, highlighting areas that need attention.

Compliance Management

Managing compliance involves adhering to legal standards and internal regulations. ADAudit Plus simplifies this imperative by offering predefined compliance reports tailored to standards such as HIPAA, GDPR, and SOX. These reports offer valuable insights into your security posture and highlight areas that need improvement.

The tool’s real-time monitoring helps in maintaining compliance by quickly identifying violations. You’ll benefit from a well-organized audit trail that documents every change made. This ongoing documentation and alert system ensures you’re always prepared for audits, leading to smoother operations and peace of mind.

Pricing and Plans

ADAudit Plus offers multiple pricing tiers to suit different organizational needs. You’ll find options ranging from a free edition to enterprise-level plans with advanced features.

Comparison of Editions

ADAudit Plus provides three main editions: Free, Standard, and Professional. The Free edition allows you to audit up to 25 workstations at no cost. Standard starts at $595 per year and includes core auditing features for AD, file servers, and workstations. Professional pricing begins at $995 annually, adding AD permissions, GPO settings, DNS, and AD schema change monitoring — and much more.

Larger organizations can benefit from the Professional edition’s scalability and comprehensive auditing capabilities. For smaller businesses, the Standard plan will be sufficient for basic monitoring needs.

Find out which plan works best for you – get a detailed quote here.

Wrapping Up

When you take a look at the ADAudit Plus for the first time, it might be a bit overwhelming given all the default reports and alerts. But spend some time filtering out what you really need. Make sure that you only get alerts for truly important events and don’t really look at the reports too much in the beginning.

ADAudit is a powerful tool, and even if you don’t have the budget for it, I recommend giving the trial and free version at least a go. It can tell you so much about your environment that it’s truly worth spending some time in it.