Reports, Features and benefits of ManageEngine ADAudit Plus

ManageEngine ADAudit Plus is a web based Active Directory change audit software. It provides comprehensive reports on almost every change that occurs in your Windows Active Directory. ADAudit Plus helps you scrutinize every change in Active Directory, while ensuring the change is in conformance with standards set by IT regulatory acts!

As the Tag line reads: Question every change – ADAudit Plus provides answers to the most important questions related to Active Directory Changes – It lets you think beyond the native Active Directory tools and scripts that are either costly or not comprehensive. ADAudit Plus provides complete data related to an Active Directory change "**Who did, what action, When and From Where**".

Who did? - Action done by a Domain User, administrator, a helpdesk technician or a malicious intruder.

What features does ADAudit Plus offer?

1. **Easy web based access:**

   ADAudit Plus is completely web based and can be accessed from anywhere in the domain. This allows centralized tracking and reporting of all audit changes.

2. **An Intuitive User Interface:**

   Self descriptive and intuitively designed user interface automatically guides users to desired results.

3. **Over 100 canned / Pre-configured reports:**

   ADAudit Plus provides over 100 pre-configured reports covering a wide variety of Active Directory audit requirements in an organization. The reports are grouped under **User Logon, Local Logon-Logoff, Account Management, User Management, Group Management, Computer Management, Domain Policy Changes, OU Management and GPO Management** categories**.** Further, the data in each report is intelligently listed under various headers of audit importance, added to this you have an Add / Remove column option for selective viewing / reporting of Audit questions.

4. **A separate Section for File Audit :**

   ADAudit Plus provides reports and alerts on the **creation, modification and deletions of Files / Folders** in a File Server. **Access** to a File Server or any **permission changes** are important changes that compliance auditors are most concerned about. This has been comprehensively addressed with a **"File Audit"** section and users can avail this benefit with the purchase of the ADAudit Plus **"File Server Add-on".**

5. **A graphical representation of various audit events via. trend analysis charts:**

   An administrator can view graphical representations of the changes to most important objects in the entire domain right from the Dashboard view of ADAudit Plus. Click on the dashboard

graphs and also view reports. They show charts through which Trends can be analyzed and also capacity expansions can be planned with a single view.

6. **Real-time alerts and Email Notifications:**

   Instant Alerts on desired / undesired audit events can be configured. These alerts are based on report profiles configured and an e-mail notification to the administrator or any selected user(s) can also be configured. This is a definitive way to monitor critical changes.

7. **Custom Reporting:**

   ADAudit Plus provides custom audit reporting capabilities; the custom reports are built over pre-configured reports by mapping specific objects of desire to the actions that are reported. (Users, Computers or groups are considered as objects in Active Directory.)

8. **Advanced configuration option to even define audit actions for select audit categories:**

   For select category of reports, make use of the Advanced Configuration ADAudit Plus option to modify any built-in audit action within ADAudit Plus. This allows you to selectively view an audit report for the action expected by you.

9. **Automated audit reporting:**

   Some audit reports in your domain are frequent events like user creation that require periodic administrator attention. These reports can be scheduled and ADAudit Plus will provide reports automatically at scheduled times, take it a step further “decide the user to be notified and configure his email for periodic email notifications of this scheduled report”.

   Multiple schedules can be created for different actions, different objects, and different time intervals.

10. **Granular reporting.**

    With the use of advanced event filtering options any administrator can make use of ADAudit Plus to view reports on specific granular actions. ***For example****: Modification to a Domain administrator account from a specific IP address.*

11. **Export:**

    Export various reports to desired formats like csv, html, pdf or xls.

12. **Archiving of audit data:**

    Archiving facility that helps maintain a secondary storage of Audit data.

13. **Enhanced efficiency through user initiated scheduled Clean-ups :**

    Schedule the Clean-up of archaic data from the working ADAudit Plus database and save precious space that complements product efficiency. ADAudit Plus allows this to be executed in a phased and organized manner – with the option to provide different intervals for different categories of audit.

14. **My Reports category that stores only the reports that are of your interest.**

    It is always an administrator's desire to view reports on only the audit events that interests him. ADAudit Plus provides an administrator option to configure "Profile based reports" and view them under a separate category – we have named it **My Reports** category.

15. **A Profile based Reports category which lists domain specific information:**

    Large organizations have multiple Domains; administrators managing such organizations would like to view Domain specific information. The profile based reports category does exactly this.

16. **Multiple users can access ADAudit Plus:**

    ADAudit Plus allows multiple technicians to access the product. Helpdesk can access the product by using operator or admin roles delegated to them. Users delegated with admin roles access the product and also manage configurations, user delegated operator roles can only view reports.

17. **Run as a Secure connection:**

    Apply your organizations' security certificate and run ADAudit Plus application as a secure connection.

18. **Efficient functioning of the application through**

    Options like

    - Event Clean-Up and Restore,
    - Diskspace Alert,
    - Alert on unsuccessful Eventlog collections
    - Delete alerts, Clear alerts

    Ensure that only the necessary audit data are held within the application for reporting / alerting needs and all other data are either cleared permanently or stored at a different location for retrieval and re-use at a later date.

Benefits of ADAudit Plus

Audit every change in Active Directory: Know the 4 dimensions of a change-'who' did 'what', 'when' and from 'where'-and ensure changes conform to organizational policies.

Supervision over crucial activities: Get prepackaged reports on crucial activities such as user logon actions and changes to GPO/OU/groups/computer/domain policies.

Unbridled Event Mining & Auditing: Using filters and rules, create your own event fetchers and engage them to collect desired event data!

Crisis Detection & Prevention: Get alerted about anomalies early on and prevent them

from magnifying into crisis.

Make IT compliance a happy experience: With incredible ease, extract any access or permission change data demanded by IT regulatory acts such as PCI, SOX, HIPAA, GLBA and FISMA.

Organized Archiving: Archive audit data for periods stipulated by IT regulatory acts and in a catalogued fashion, so that regeneration of reports becomes easy.

Forensics & Incident Prevention: Study the archived process information, get to the root of any problem and prevent it from re-emerging!

What actions are audited by ADAudit Plus?

ADAudit Plus provides a host of reports that are categorically listed under 9 different categories.

Each category shows reports as listed below:

Reports	Functions
User Logon Reports	
Logon Failures	This category of reports provides data on all logon information that are recorded in the configured Domain Controllers. Logon information of a specific user in the domain, Logon into a specific computer and last logon on a workstation are reported.
Domain Controller Logon Activity	
Member Server Logon Activity	
Workstation Logon Activity	
User Logon Activity	
Recent User Logon Activity	
Last Logon on Workstations	
User's Last Logon	
Local Logon-Logoff	
Logon Duration	Reports dependent on the local Logon audit data can be viewed from this section. ADAudit Plus provides Local Logon data for Domain Controllers and Member Servers. **Local Logon:** Data recorded in the security log of that specific computer. Both Logon and Logoff data is possible.
Logon Failures	
Logon History	
Terminal Services Activity	
Account Management	
User Management	This section of reports helps one to audit the use of admin authority to execute management tasks in the organization. Use of admin authority for User, Group, Computer, OU and GPO management tasks can be audited.
Group Management	
Computer Management	
OU Management	
GPO Management	
User Management	
Recently Created Users	This category of reports enables you to audit all recently created, deleted or modified users in the domain.
Recently Deleted Users	
Recently Enabled Users	

Recently Disabled Users	
Recently Locked Out Users	
Recently Unlocked Users	
Recently Password Changed Users	
Recently Password Set Users	
Password Never Expires Set Users	
Recently Modified Users	
Last Modification on Users	
Administrative User Actions	
User Object History	
Group Management	
Recently Created Security Groups	Creations, deletions or modification to all Security and Distribution Groups in the domain can be audited. Additions or deletions of members to these groups are pointed out. History of changes to a group is listed in detail.
Recently Created Distribution Groups	
Recently Deleted Security Groups	
Recently Deleted Distribution Groups	
Recently Modified Groups	
Recently Added Members to Security Groups	
Recently Added Members to Distribution Groups	
Recently Removed Members from Security Groups	
Recently Removed Members from Distribution Groups	
Group Object History	
Computer Management	
Recently Created Computers	This section is an audit trail of computer objects in your network. Right from creation of a computer object to deletion, every action is reported. Even the changes done to a computer object are recoded and reported. A complete history of modifications carried out on one or more computer objects is listed under this category.
Recently Deleted Computers	
Recently Modified Computers	
Recently Enabled Computers	
Recently Disabled Computers	
Computer Object History	
Domain Policy Changes	
Domain Policy Changes	Account policy and password policy changes are audited and reported.
OU Management	
Recently Created OUs	Any change related to creation, deletion or modification of an Organizational Unit is audited and reported. Audit data on the history of changes to an OU is also reported.
Recently Deleted OUs	
Recently Modified OUs	
OU History	
GPO Management	
Recently Created GPOs	GPO (Group Policy object) creations, deletions, modifications and also GPO Link changes can be audited with the reports listed under this section.
Recently Deleted GPOs	
Recently Modified GPOs	

GPO Link changes	
GPO History	

File Audit Reports:

File Audit has been comprehensively addressed by ADAudit Plus. While most competitors provide this as a separate product, ADAudit Plus has made it available as an add-on, thus allowing end-users to comprehensively view audit data within a single comprehensive audit solution.

File Audit Reports are listed under 3 separate categories.

1. **Comprehensive File Audit Reports**
2. **Server Based Reports**
3. **User Based Reports**

Further **Profile Based Reports** and **My Reports category** a highlight of ADAudit Plus are also available.

Provided below is a list of File Audit Reports provided by ADAudit Plus.

Reports	Functions
File Audit Reports	
All File or Folder Changes	This category of reports provides data on Windows File Server Audit. The reports are displayed under 3 categories for easier interpretation of FILE AUDIT DATA. You can also customize the reports and view them as Profile Based Reports or My Reports.
Files Created **Files Modified** **Files Deleted**	
Successful File Read Access **Failed attempt to Read File**	
Failed attempt to Write File **Failed attempt to Delete File**	
Folder Permission Changes	
Folder Audit Setting Changes(SACL)	