

# ManageEngine ADAudit Plus

## ADAudit Plus Quick Start Guide

### Contents

#### Introduction :

What is ADAudit Plus?  
How ADAudit Plus works?  
With ADAudit Plus you can

#### Setup :

Installation  
System Requirements  
Storage Requirements

#### Check List :

Ports need to opened  
Configuring audit policies  
Security log settings  
Permissions required for ADAudit Plus

## Introduction

### What is ADAudit Plus ?

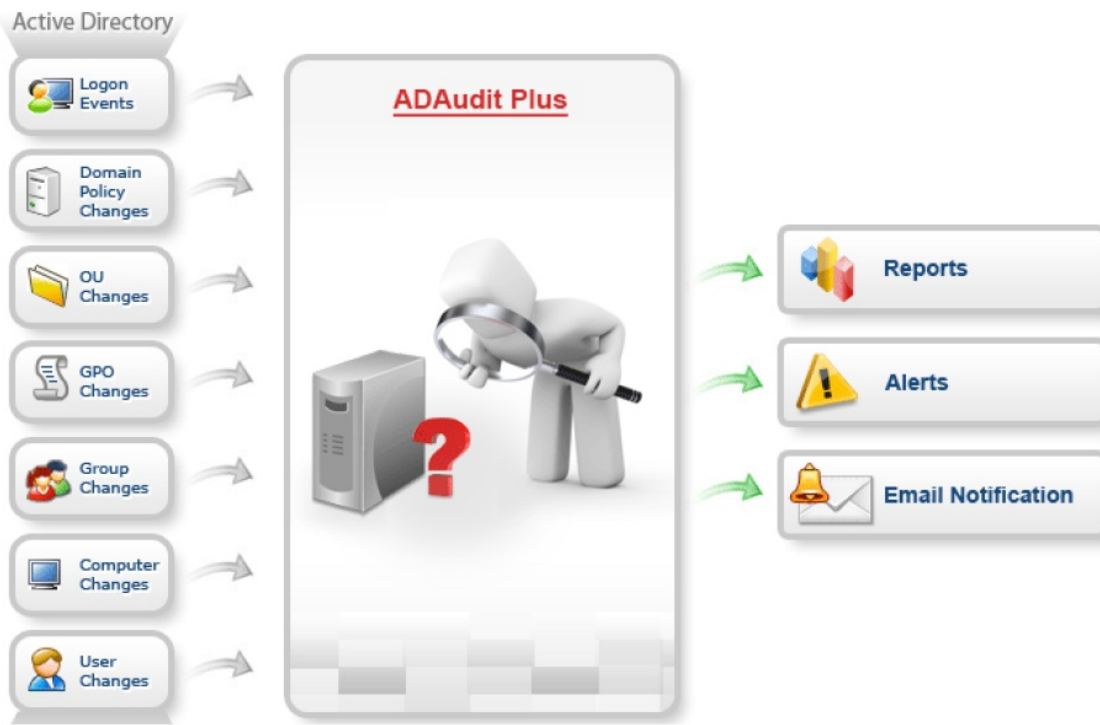
ADAudit Plus is an enterprise-wide Active Directory & File Server change auditing software with reports and alerts that:

- Addresses the most-needed security, audit and compliance demands set forth by regulatory and government bodies.
- Provides an IT administrator the right business add-ons to assist in the execution of a change management action.

The solution provided by ADAudit Plus are in the form of comprehensive reports and alerts, which are easily comprehensible even to technically naive users. The reports answer the four vital W's of Active Directory auditing: "Who" did "what" action, "when" and from "where"!

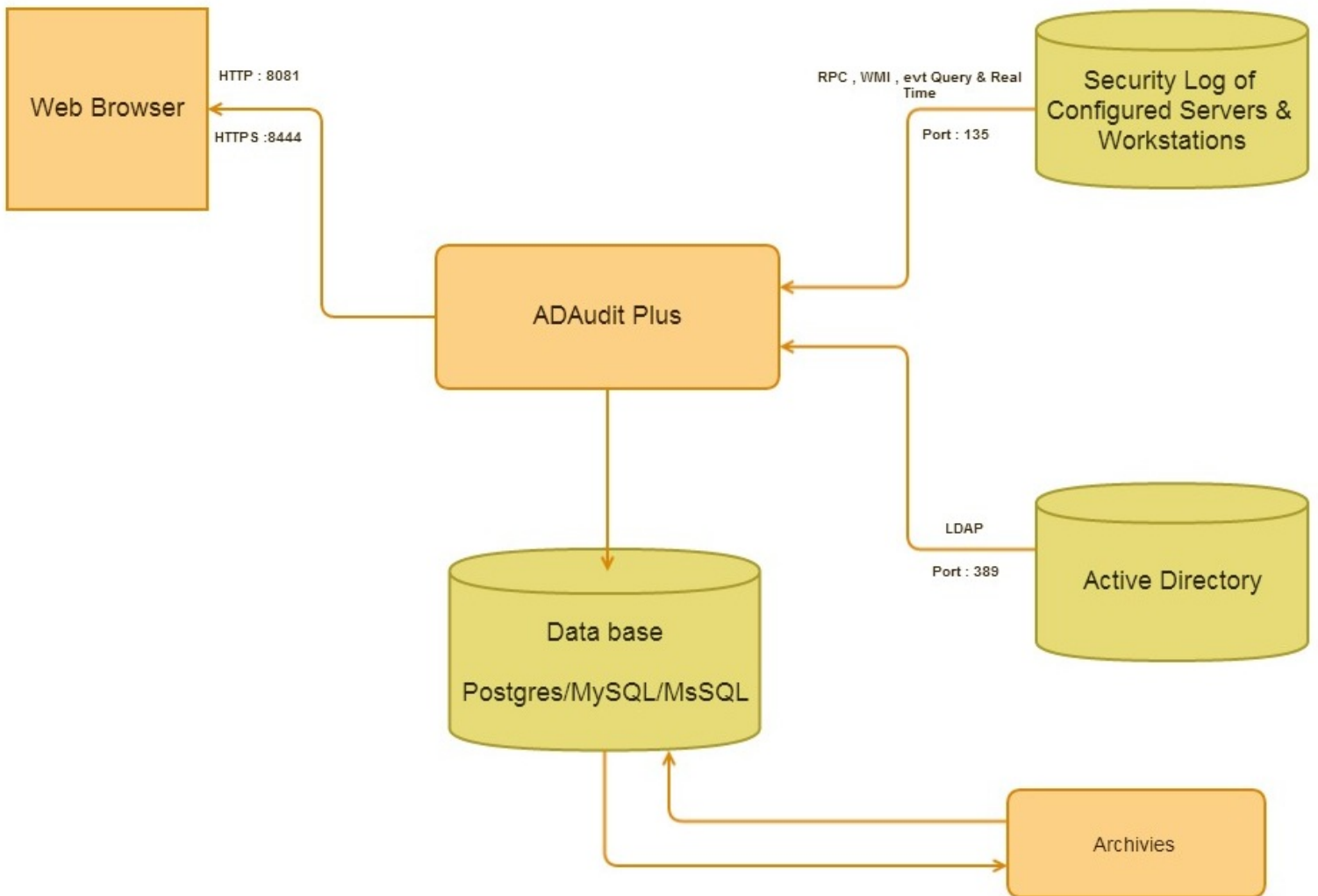
The audit solution not only shows data related to a change, but also allows the export of results to xls, html, pdf and csv formats and provides the option to print listed data which to assist in interpretation.

### How ADAudit Plus works ?



ADAudit Plus works on the basis of native auditing. Audit policies and SACLs must be configured on the Domain Controllers and Member servers to enable auditing. This ensures that all changes made to Active directory, Logon activities gets logged in the security log of the respective servers. ADAudit Plus collects these events to report on changes.

### Technology flow of ADAudit Plus



# Setup

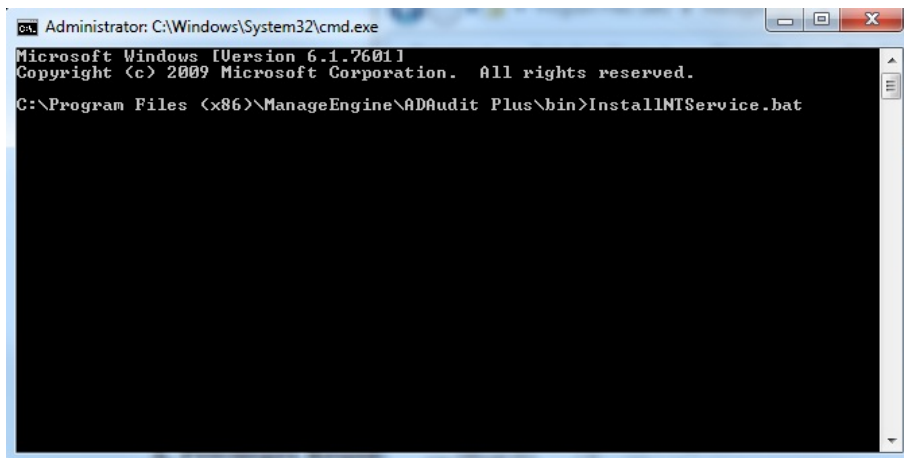
## Installation

ADAudit Plus is distributed in the EXE format. ADAudit Plus can be installed in any machine in the domain with the specified system requirements. ADAudit Plus can be installed on any computer on the network and can be accessed from any client computer on the network using a web browser.

### ADAudit Plus as windows service :

Follow the steps below to run ADAudit Plus as Windows service.

- Stop ADAudit Plus(Start->All Programs->ADAudit Plus->Stop ADAudit Plus).
- Open the command prompt (Right Click --> Run as administrator In case of Windows server 2008)
- Goto <Installation Folder>ADAudit Plus\bin [eg : C:\Program Files (x86)\ManageEngine\ADAudit Plus\bin ]
- Execute "InstallNTService.bat"



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Program Files (x86)\ManageEngine\ADAudit Plus\bin>InstallNTService.bat
```

- Open the services.msc -->"ManageEngine ADAudit Plus" Service --> Right click --> Properties
- Click on "Log on" tab and select the "This Account" and provide the credential ( If possible, use an admin account).
- Start ManageEngine ADAudit Plus

## System Requirements

### Hardware Requirements :

Hardware	Recomended
Processor	P4 - 1.5 GHz or better
RAM	2 GB or better

<b>Disk Space</b>	<b>20 GB</b>
-------------------	--------------

Note : The additional disk space used by database will vary depending on the number of Users / Files and audited events captured.

**Software Requirements :**

**Supported Operating Systems** - ManageEngine ADAudit Plus can be installed and run on the following Microsoft Windows operating system versions:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 2003 Server
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

**Supported Browsers** - ManageEngine ADAudit Plus requires one of the following browsers to be installed in the system

- Internet Explorer 6 and above
- Firefox 2.0 and above
- Chrome
- Preferred screen resolution 1024 x 768 pixels or higher

**Supported Platforms :**

- Active Directory 2003 and above
- Windows File Server 2003 and above
- NetApp Filer - Data ONTAP 7.2 and above
- Windows Failover Cluster with SAN

**Storage Requirements :**

**Active Directory Auditing :**

No. of Users	No. Of Days	Total size
1	1	15 KB
10,000	90	12*10000*90 = 13 GB

## File Server Auditing :

No. of Users	No. of Files	No. of Days	Total size
1	1	1	4 KB
100	1	1	400 KB
100	100	1	40 MB
100	100	90	40000*90 = 3.5 GB
100	100	720 (2 Yrs)	40000*720 ~ 29 GB

## Check list

### Ports need to opened

### For event collection :

- Port "389" to communicate with the LDAP Protocol
- Port "135" to communicate with RPC
- Port "445" and "135" to communicate with NetBioS Session Service

### To access ADAudit Plus :

- http : 8081
- https : 8444

### Configuring audit policies

Audit Policies must be configured in any Active Directory environment; this ensures that relevant audit data are logged into the security logs of desired computers / domain controllers. ADAudit Plus will be able to collect and report audit data only for audit policy enabled computers.

### To audit Active Directory

1. The Default Domain Controller policy must be configured.
2. Object-Level Auditing should be enabled.

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/manual-configuration-dc-auditing.html>

<http://www.manageengine.com/products/active-directory-audit/help/reports/access-audit-to-enable-audit-sacls.html>

### **To audit File Servers**

1. Audit Policy must be configured for the specific File Servers from where audit data is required.
2. Object-Level Auditing should be enabled

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/configure-object-access-auditing.html>

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/linking-servers-to-gpo.html>

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/sacls-to-audit-files-and-shares.html>

### **To audit Member Servers**

Audit Policy must be configured for the specific Member Servers from where audit data is required.

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/configure-local-log-auditing.html>

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/configure-policy-member-server-auditing.html>

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/linking-servers-to-gpo-ms.html>

### **Enabling File Integrity Monitoring [Member Servers]**

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/fim-audit-policy.html>

### **To Audit NetApp Filers**

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/netapp-filer-manual-configuration.html>

<http://www.manageengine.com/products/active-directory-audit/help/getting-started/sacls-to-audit-files-and-shares.html>

Advanced audit policy configuration for 2008 R2 and above Domain Controllers and Member Servers

DC Auditing	Member Server Auditing	File Server Auditing	Workstation Auditing
<p><b>Account Logon</b></p> <ul style="list-style-type: none"> <li>* Kerberos Authentication Service(S &amp; F)</li> </ul> <p><b>Account Management</b></p> <ul style="list-style-type: none"> <li>*Computer Account Management(S)</li> <li>*Distribution Group Management(S)</li> <li>*Security Group Management(S)</li> <li>*User Account Management(S &amp; F)</li> </ul> <p><b>Detailed Tracking</b></p> <ul style="list-style-type: none"> <li>*Process Creation(S)</li> <li>*Process Termination(S)</li> </ul> <p><b>DS Access</b></p> <ul style="list-style-type: none"> <li>*Directory Services Changes(S)</li> <li>*Directory Service Access(S)</li> </ul> <p><b>Logon/Logoff</b></p> <ul style="list-style-type: none"> <li>*Audit Logon(S &amp; F)</li> <li>*Audit Logoff(S)</li> <li>*Network Policy Server(S &amp; F)</li> <li>*Other Logon/Logoff Events(S)</li> </ul> <p><b>Object Access</b></p> <ul style="list-style-type: none"> <li>*Other Object Access Event(S)</li> </ul>	<p><b>Account Management</b></p> <ul style="list-style-type: none"> <li>*Computer Account Management(S)</li> <li>*Distribution Group Management(S)</li> <li>*Security Group Management(S)</li> <li>*User Account Management(S &amp; F)</li> </ul> <p><b>Detailed Tracking</b></p> <ul style="list-style-type: none"> <li>*Process Creation(S)</li> <li>*Process Termination(S)</li> </ul> <p><b>Logon/Logoff</b></p> <ul style="list-style-type: none"> <li>*Audit Logon(S &amp; F)</li> <li>*Audit Logoff(S)</li> <li>*Network Policy Server(S &amp; F)</li> <li>*Other Logon/Logoff Events(S)</li> </ul> <p><b>Object Access</b></p> <ul style="list-style-type: none"> <li>*Other Object Access Event(S)</li> </ul> <p><b>Policy Change</b></p> <ul style="list-style-type: none"> <li>*Authentication Policy Change(S)</li> <li>*Authorization Policy Change(S)</li> <li>*Audit Policy Change(S)</li> </ul> <p><b>System</b></p> <ul style="list-style-type: none"> <li>*Security State Change(S)</li> </ul>	<p><b>Logon/Logoff</b></p> <ul style="list-style-type: none"> <li>*Audit Logon(S &amp; F)</li> <li>*Audit Logoff(S)</li> <li>*Network Policy Server(S &amp; F)</li> <li>*Other Logon/Logoff Events(S)</li> </ul> <p><b>Object Access</b></p> <ul style="list-style-type: none"> <li>*File System(S &amp; F)</li> <li>*Handle Manipulation(S &amp; F)</li> </ul>	<p><b>Logon/Logoff</b></p> <ul style="list-style-type: none"> <li>*Audit Logon(S &amp; F)</li> <li>*Audit Logoff(S)</li> <li>*Network Policy Server(S &amp; F)</li> <li>*Other Logon/Logoff Events(S)</li> </ul>



<b>Policy Change</b>  *Authentication Policy Change(S) *Authorization Policy Change(S)  <b>System</b>  *Security State Change(S)			
---	--	--	--

### Security log settings

ADAudit Plus periodically collects the audit-data from the configured servers and stores the information in the database for reporting. To avoid data loss, we recommend the below Event Log Settings.

Operating System Of Server	Role	Security Log size (Kb)	Security Log Retention
Windows Server 2003	Domain Controller	307200	Overwrite Events As Needed
Windows Server 2008 and above	Domain Controller	1048576	Overwrite Events As Needed
Windows Server 2003	File Server	307200	Overwrite Events As Needed
Windows Server 2008 and above	File Server	4194304	Overwrite Events As Needed
Windows Server 2003	Member Server	307200	Overwrite Events As Needed
Windows Server 2008 and above	Member Server	1048576	Overwrite Events As Needed

### Permissions required for ADAudit Plus

ADAudit Plus required certain privileges to collect events from the configured servers to report on changes. Please click on the below link to find the complete details of privileges required for ADAudit Plus to collect audit data from the configured servers.

<http://www.manageengine.com/products/active-directory-audit/audit-permissions-configuration-ad-audit-plus.html>

## **ADAudit Plus Admin Configuration [Admin Tab]**

### **Alert Me :**

The "Alert Me" feature continuously monitors if ADAudit Plus is collecting event-log data from the security logs of configured servers. It sends an email alert to the configured email address when ADAudit Plus stops collecting event-log data.

The function also monitors the drive on which ADAudit Plus is installed and alerts when the free space drops below a set threshold. It also alert on License expiry.

### **Technician/Operator :**

The mere size of an organization makes it all the more difficult for a single administrator to monitor all changes that occur in the network. There is a need to delegate monitoring roles to one or more users in the domain and this can be effectively established using the technician delegation feature in ADAudit Plus.

ADAudit Plus allows delegation for two different roles:

1. Admin Role : The admin role will have complete privileges to the ADAudit Plus settings and configurations.
2. Operator Role : The operator roles will have privileges only to view reports, alerts and graphs configured by the administrator.

### **Exclude User Accounts :**

A service account is a Active Directory user account that is created explicitly to provide a security context for services running on Windows Server. And this account generates huge amount of logon events and which in-turn consume a huge amount of space in the database and alerts from these accounts prove to be a waste of an administrator's time.

To Exclude User Accounts:

1. Click on Admin Tab
2. Select "Exclude User Accounts" under Administration
3. Select the Domain (This displays the list of all user accounts in the domain under "Available Users")
4. Exclude one or more users from the Available Users list by using >> option.
5. Click on Save.

#### **Exclude Configuration in File Audit :**

The File Audit Feature helps audit all types of access(read, write, delete and permission changes to the files in File Server). The read access audit includes both manual read access and Process read access, here the process states the Backup Scans and other automated scan. And this automated process will generate enormous amount of File Read Events and which in-turn consume a huge amount of disk space and alerts from these accounts prove to be a waste of an administrator's time.

To Exclude a specific Process/Users/File Types from File Auditing :

1. Click on File Audit Tab
2. Select "Exclude Configuration" under Configuration
3. Specify the name of the Process/File Type separated by commas
4. Click on Save.

#### **Need for Archiving:**

The need for archiving does not stop with compliance. Archived data is very important for organizations in-order to:

- Help with the Forensic analysis and reporting.
- Ensure the audit data that might be required for various compliance needs are safe and unaltered. (Compliance requirements like SOX, HIPAA, GLBA etc., demand audit log data for a minimum period of 3 years or more.)
- Analyze Microsoft Windows Active Directory/File Server/Member Server unauthorized attempts that have led to a lapse in internal security and also in maintaining an already established internal organizational policy.
- Plan resource capacity by studying resource utilization patterns for various periods. Isolate suspicious users (user logon data) and corroborate their involvement in any past security attack with the use of their audit trails.

## **Regeneration of archive data, the ADAudit Plus advantage:**

ADAudit Plus advantages, that help in the regeneration of archived data include:

- Allows audit data to be archived at a user defined location, this can be a storage server anywhere within the network.
- Helps you to archive only the desired Active Directory change data, thereby reducing the clutter normally associated with native methods of secondary storage.
- Follows a catalogued relegation of individual journals of change data, grouped into multiple compressed files, earmarked by event occurrence dates. These compressed files contain filtered log information stored in an unadulterated format.
- The journal data is stored in a format that allows for restoration and regeneration as and when demanded and for desired period.

### **To enable Archiving:**

- Click on the "Admin" Tab --> "Archive Events" under "Administration"
- Provide a check against desired categories and enter the "days" older than which the processed data will be cleared from the immediate database and archived.

This archived data can be easily restored and used by ADAudit Plus application for “custom reporting”, where users determine the reporting period. Custom reporting for any older date is always possible in ADAudit Plus with this restored data. Such custom reports play a vital role in forensics, security, and compliance auditing.

## **HTTP/HTTPS**

All communications between ADAudit Plus and client communication happens via a simple and self explanatory web browser interface. These server-client interactions happen in HTTP protocol by default. While ADAudit Plus and client communication via HTTP may be safe in a closed LAN, you **MUST** implement HTTPS protocol between ADAudit Plus and clients, if the client is situated outside a LAN and would use internet to access ADAudit Plus. In cases like geographically disparate WAN or use over internet, please apply enable SSL Port (https), so that client-server communication is encrypted.

Procedure :

1. Click on Admin tab -->> Connection settings.
2. Check in the Enable ssl port [https] to enable secure sockets layer and enter the number.
3. Click on save changes.

## With ADAudit Plus You can

### Active Directory Auditing:

- \* [Active Directory audit reports](#)
- \* [User logon audit reports](#)
- \* [Tracking user management actions](#)
- \* [User management audit reports](#)
- \* [All AD Change Audit Reports](#)
- \* [Active Directory alerts and email notification](#)
- \* [Active Directory audit and compliance](#)
- \* User Logon and Log-Off
- \* Account Lockout analyzer
- \* DNS Auditing
- \* Schema Auditing
- \* Permission Changes
- \* Real Time Reports and Alerts - 2008 and above DC [New]

### GPO Changes :

- \* [GPO change auditing](#)
- \* [Advanced GPO audit reports](#)

### Member Server Auditing :

- \* [Logon/Logoff](#) (Domain and Local), Logon Duration on Member Server and Workstations
- \* Terminal Services Activity
- \* Schedule Tasks Activity
- \* System Changes - Start/Stop/Audit Log cleared
- \* Process Tracking on Servers.
- \* [Printer auditing](#) [New]
- \* [File Integrity Monitoring](#) [New]

### File Server Auditing :

- \* [File/Folder Creation, Modification, Deletion](#) (Success and Failed attempt)
- \* File Read Access (Success and Failed attempt)
- \* Folder Permission Changes.
- \* Folder Audit Settings Changes (SACL)"
- \* File move/Rename
- \* File Copy action

### NetApp Filer Auditing :

- \* [File/Folder Creation, Modification, Deletion](#) (Success and Failed attempt)

- \* File Read Access (Success and Failed attempt)
- \* Folder Permission Changes.
- \* Folder Audit Settings Changes (SACL)"
- \* File move/Rename

#### EMC Auditing [**New**] :

- \* [File/Folder Creation, Modification, Deletion](#) (Success and Failed attempt)
- \* File Read Access (Success and Failed attempt)
- \* Folder Permission Changes.

#### Reporting :

ADAudit Plus has a plethora of reports to audit your Active Directory efficiently from anywhere in the domain. ADAudit Plus reports can be accessed by selecting the Reports tab from the client window they are grouped under the following categories by default.

Features that are common to all the Reports:

- Generate reports for multiple domains.
- Customizable columns by using the Add / Remove Column link available in all the reports this
- allows to select additional attributes to the list of already available attributes that are displayed in the report.
- Perform a quick search by inputting any attribute value that is displayed in the columns.
- Add to Favourites - Pre-defined reports with user inputs can be bookmarked and scheduled
- Columnar sorting of reports
- Ability to print the reports.
- Reports can be exported to CSV, PDF, XLS and HTML formats.
- Option to View Reports based on listed and Custom Selected Time Periods.
- Add your own annotations to be displayed while export using the annotation link.
- Each Report has a Graphic display to help access more granular audit information with ease.
- Option to select the number of rows that are to be displayed in a single page of a report.
- Reports can be stored in any of the following formats 'pdf', 'xls', 'csv', or 'html'.
- One or more reports can be selected and [scheduled](#) to be run at user selected times and also
- emailed to one or more user email ids.

#### Alerts :

With ADAudit Plus, you can configure and view alerts for a specific change event. For example: You can configure and view an alert for a failed logon on a specific computer in the Domain.

#### To create a New Alert Profile :

- Click on "Configuration" Tab -->"Create Alert Profile" under Alert Profiles.
- This displays the Create Alert Profile Page.

- Enter the "Name" of the Alert Profile in the Box Provided.
- Enter the "Description" of the Alert Profile in the Box Provided.
- Select the "Severity" of the Alert Profile (The Severity depends on importance of the Alert and can indicate "Attention, Trouble, or Critical")
- Select the "Report Profile" for a Domain
- Click the "Plus" icon to the right of Report Profile Box a Pop-up appears.
- Select the "Domain" from the Drop Down.
- Select the "Category" from the Drop Down.
- Select one or more of the available "Report Profiles" to be alerted by providing a check against them.
- Click on OK.
- To add an Alert Message Click on the [Add] link to the right of Alert Message Box. The "Alert Message" can be typed with a common alert message or customized alert messages can also be configured. Click on "OK".
- To Send Email Notifications provide a check against the "Send E-mail Notification" Check Box and Enter the recipient Email addresses in the box provided.
- Click on "Save"
- A new Alert Profile is created.

#### **Custom Reports & Alerts :**

Report Profile based reports which can be custom configured is an advanced feature. This is a highlight of ADAudit Plus which facilitates reporting to granular detail by using filters. Change audit events are reported by associating audit actions and one or more account objects with report profiles and facilitate granular reporting. The advantage of using a Report Profile based report makes the process of granular report generation on audit actions easier.

**ADAudit Plus Team**  
**Active Directory & File Server Auditing with ADAudit Plus**  
**Email : support@adauditplus.com**  
**DID : +1-408-916-9891**  
**Toll free: +1-888-720-9500**

