

Make sure you keep
a track of who does what
change when and from where.

Help Document



Table of Contents

WELCOME TO ADAUDIT PLUS	3
Release Notes	4
Contact ZOHOO Corp.	5
ADAUDIT PLUS TERMINOLOGIES	7
GETTING STARTED	8
System Requirements	9
Installing ADAudit Plus	10
Working with ADAudit Plus	11
Licensing ADAudit Plus	13
Configuring Audit Policy Settings.....	14
Configuring SACLs for GPO and OU Objects	16
Dashboard View	19
REPORTS	20
User Logon Reports.....	21
User Management	25
Group Management.....	30
Computer Management.....	34
Group Policy Objects (GPO) Management Audit Reports.....	37
Organizational Units Management Audit Reports.....	39
Profile Based Reports.....	42
Schedule Reports	44
ALERTS	47
CONFIGURATION	50
Report Profiles	51
Alert Profiles	54
Audit Actions.....	58
Advanced Configurations.....	59
ADMIN	65
General Settings	66
Personalize	67
Connection.....	68
Server.....	69
Mail Server Settings.....	70

Administration	71
Domain Settings.....	72
Alerts	74
Schedule Reports	75
Archive Settings	78
Event Cleanup	79
Technician Settings.....	80
TROUBLESHOOTING TIPS.....	81
KNOWN ISSUES AND LIMITATIONS.....	83

Welcome to ADAudit Plus

A growing need to manage accounts in an organization necessitates an administrator to delegate roles to helpdesks, support staffs, Human Resource and other Users. The privileges that are delegated include user management, Group Management, Computer Management and others. With Administrator privileges distributed across different users in the domain there is a need to have information on Who did an activity, When was it done, Where was it done from, On Whom and what the action was performed.

The Who, Where and When information is very important for an administrator to have complete knowledge of all activities that occur on his Active Directory. This helps him identify any desired / undesired activity happening. ADAudit Plus assists an administrator with this information in the form of reports.

Audit and compliance requirements are becoming mandatory with stricter security requirements imposed by various governments and organizations worldwide. Further IT Administrators require reports and alerts on change actions done by users which are important for security. ADAudit Plus has a plethora of reports to audit any change that occurs in Active Directory. These Reports can be configured to suit an administrator's need. ADAudit Plus not only reports on activities done by users but also facilitates alerts. Alerts can be configured to specify the severity of attention that an action done necessitates.

Alerts / Reports from ADAudit Plus can be configured based on need. Further an administrator can define an activity to be a combination of rules and rule groups. ADAudit Plus facilitates custom reports or report profile configuration which facilitates the reporting mechanism to be customized to the users need. A report profile can be customized by restricting the report to be associated with selected domains, organizational units, domain controllers or objects in the Active Directory.

A Dashboard view for easy interpretation of most important Change Actions done in various domains. Multicolor Charts and Graphs to differentiate various change Audit Actions. Customizable report views with addition and removal of desired columns are an highlight of ADAudit Plus. These features makes ADAudit Plus easy to understand software and the audit information extracted to be meaningfully used during audits or to perform any corrective action.

Release Notes

ADAudit Plus is a web based Active Directory Change Auditing and Reporting Solution. It helps an administrator to take decisions based on change information on users, computers, groups, contacts, Logon, domain policies and more by extracting change or audit information from the event viewer of the Domain Controllers. The reports are easy to understand and can be generated by associating domain objects and Actions.

The key features of this release ManageEngine ADAudit Plus 4.0.0 Build Number:4030 include

New Features

- Multi-user login capabilities - Allow multiple users to login into the ADAudit Plus web portal. Admin users with complete privileges and operator users with read only privileges can be delegated.
- GPO Auditing : Creation, Modification, Deletion of GPO's, GPO link changes and GPO change history are reported.
- OU Auditing : Creation, Modification, Deletion of OU's, and OU history are reported.

Enhancements

Additional Pre-configured Reports on

- Additional Pre-configured reports, "Recently modified groups", "Password never expires", "User's last logon" and more.
- Event Log Properties of Domain Controllers can be viewed from "Domain Settings" page.
- Some bug fixes, configuring mail server with user credentials, multi-user selection in IE6 fixes etc.,

Contact ZOHO Corp.

- ZOHO Corp. Headquarters
- Sales
- Technical Support

ZOHO Corp. Headquarters

Web site	www.zohocorp.com
ZOHO Corp. Headquarters	<p>ZOHO Corp. 5200 Franklin Dr, Suite 115 Pleasanton, CA 94588 USA Phone: +1-925-924-9500 Fax : +1-925-924-9600 E-mail: info@manageengine.com</p>
ZOHO Development Center	<p>ZOHO Development Centre (I) Private Limited 11 Sarathy Nagar, Vijayanagar, Velachery, Chennai 600 042 INDIA Phone: +91-44-22431115 (10 lines) Fax: +91-44-22435327 E-mail: info@manageengine.com</p>

Sales

To purchase ManageEngine ADAudit Plus from any part of the world, you can fill out the Sales Request Form. A sales person will contact you shortly. You can also send us an email at sales@manageengine.com.

You can also call the ZOHO Corp. headquarters at the following numbers:

Phone: +1-925-924-9500
 Fax : +1-925-924-9600 and request for Sales

Technical Support

One of the value propositions of ZOHO Corp. to its customers is excellent support. During the evaluation phase the support program is extended to you free of charge. Please send your technical queries to support@adauditplus.com

Following is the support format to be enclosed, while sending support mails:

- Edition (Free or Standard Edition) of the product
- Operating System version, such as Win 2000, 2003, etc.
- Browser version, such as Netscape 7.0, IE 5.5, etc.
- Details of the problem
- Steps to reproduce the problem.

Alternatively, select the Support tab from the client window. It has the following options that will allow you to reach us:

- Request Support - Submit your technical queries online.
- Need Features - Request for new features in ADAudit Plus.
- User Forums - Participate in a discussion with other ADAudit Plus users.
- Contact Us - Speak to our technical team using the toll free number (1-888-720-9500)

ADAudit Plus Terminologies

Terminologies Used in ADAudit Plus

ADAudit Plus follows terminologies specific to the product. We have defined some of the commonly used terminologies in this page for easy understanding of the Product.

The Generally used Terminologies in ADAudit Plus Include

1. Report Profile
2. Alert
3. Activity
4. Event
5. Audit Actions
6. Category

Report Profile:

Methodology to filter the necessary events from Event data, and associate them to Active Directory Objects like users, computers, groups etc.,

Alert:

An alarm on the high priority event when it happens. Alerts can be scheduled and automatically delivered via. email.

Activity:

Any action that is performed in an Active Directory like, creating a user, deleting a user, adding a member to a group, logging into a machine etc.,

Event:

Data stored by Microsoft as event logs on activities performed in Active Directory when the Auditing Policy is enabled.

Event Number:

For every activity that is completed an event number is recorded in the Eventlog. Microsoft logs in each event with a specific number and stores the information in the Eventlog of the Active Directory. This event number is critical for Auditing Purposes – ADAudit Plus identifies and reports Audit Activities based on the Event Numbers.

Audit Actions:

Rules formulated to filter the necessary events from the Event Data.

Category:

Categorization of Event Logs depending on each activity which is similar to the "Category" in Event Viewer. Eg., Account Logon, Account Management etc.,

Getting Started

This section describes on how to get started with ADAudit Plus.

- System Requirements
- Installing ADAudit Plus
- Working with ADAudit Plus
- Licensing ADAudit Plus

System Requirements

- Hardware Requirements
- Software Requirements

Hardware Requirements

Hardware	Recommended
Processor	P4 - 1.0 GHz
RAM	512 MB
Disk Space	800 MB

Software Requirements

Supported Platforms

ManageEngine ADAudit Plus supports the following Microsoft Windows operating system versions:

- Windows Server 2000.
- Windows XP.
- Windows Server 2003.
- Windows Vista.

Active Directories supported : Windows Server 2000 and Windows Server 2003.

Supported Browsers

ManageEngine ADAudit Plus requires one of the following browsers to be installed in the system for working with the client.

- Internet Explorer 6.0 and above
- Firefox 2.0 and above

Preferred screen resolution 1024 x 768 pixels or higher.

Installing ADAudit Plus

- Installing ADAudit Plus
- Uninstalling ADAudit Plus

Installing ADAudit Plus

ADAudit Plus is distributed in the EXE format. ADAudit Plus can be installed in any machine in the domain with the specified system requirements. You can install ADAudit Plus as:

- An Application
- A Windows Service

Installing ADAudit Plus as an Application

By Default ADAudit Plus will be installed as an application, run the self-extracting EXE and follow the instructions.

When ADAudit Plus is installed as an Application, starting ADAudit Plus runs with the privileges of the user who has logged on to the system.

ADAudit Plus as a Windows Service

To run ADAudit Plus as a service. Do the following steps after installing.

1. Go to Start Menu
2. All Programs
3. Select ADAudit Plus
4. Select NT Service
5. Select Install ADAP Service

When ADAudit Plus is installed as a service, starting ADAudit Plus runs with the privileges of the system account.

Uninstalling ADAudit Plus

To uninstall ADAudit Plus , Stop ADAudit Plus and then Un-install the Program

To Stop the Application

Select **Start --> Programs --> ADAudit Plus --> Stop ADAudit Plus Server**

To Uninstall

Select **Start --> Programs --> ADAudit Plus --> Uninstall ADAudit Plus.**

Working with ADAudit Plus

- Starting ADAudit Plus
- Launching ADAudit Plus Client
- Stopping ADAudit Plus

Starting ADAudit Plus

ADAudit Plus can be started either in the system account (when run as service) or in user account (when run as application).

When ADAudit Plus is not installed as a Service

In this case, ADAudit Plus can only be started in the user account

To start the product,

Select **Start --> Programs --> ADAudit Plus --> Start ADAudit Plus** (or) double-click the ADAudit Plus desktop icon.

When ADAudit Plus is installed as a Service

Installing ADAudit Plus as a service allows it to be started from the system account.

To start ADAudit Plus service,

Click on **Start --> Control Panel --> Administrative Tools --> Services --> Start the Service "ManageEngine ADAudit Plus"**

On starting the ADAudit Plus, the client is automatically launched in the default browser.

When ADAudit Plus is started in Windows XP / Windows 2003 machines with firewall enabled, Windows may pop up security alerts asking whether to block or unblock the following programs as shown in the images below:

1. mysqld-nt - Database server
2. Java(TM) 2 Platform Standard Edition binary - Java.

You should Unblock these programs to start ADAudit Plus.



Fig: MySQL Alert



Fig: Java Alert

Launching ADAudit Plus Client

To launch the ADAudit Plus client,

1. open a Web browser and type `http://hostname:8081` in the address bar. Here the hostname refers to the DNS name of the machine where ADAudit Plus is running.
2. Specify the user name and password as admin (for first time users) in the respective fields and click Login. If you have changed the password, you should use the changed password to login.

Stopping ADAudit Plus

To stop ADAudit Plus, select **Start --> Programs --> ADAudit Plus--> Stop ADAudit Plus**

Licensing ADAudit Plus

ADAudit Plus is available in two editions - Free and Standard Editions

Download the product from the Website

<http://www.manageengine.com/products/active-directory-audit/download.html>.

The Free Edition and the Standard Edition, come packaged as a single download. During the evaluation phase, the Standard Edition is installed and can be evaluated for 30 days. After 30 days, it is automatically converted to the Free Edition, unless the Standard Edition license is purchased.

- Restrictions in Trial Edition
- Restrictions in Free Edition
- Licensed Version of ADAudit Plus
- To upgrade from a Trial Edition or Free Edition to Standard Edition

Restrictions in Trial Edition

ADAudit Plus is licensed based on the number of Domain Controllers enabled. The trial edition is limited to fetching event data from 5 Domain Controllers.

The following are the restrictions in the Trial Edition:

1. Any Number of Domains or Domain Controllers can be Added.
2. Event Data is fetched only from 5 Domain Controllers.
3. Additional Domain Controllers can be added but will be in a Disabled State and Data Collection will not happen from these Domain Controllers.

Restrictions in Free Edition

The following are the restrictions in the Free Edition:

1. Fresh Event Data will not be fetched from Domain Controllers.
2. Only data last fetched during the trial / licensed period is reported and can be used.

Licensed Version of ADAudit Plus

ADAudit Plus is licensed based on the number of Domain Controllers enabled.

1. The licensed version of ADAudit Plus is fully functional and can fetch event data from the licensed number of Domain Controllers.
2. Both Historical and Real-time reporting is possible.
3. Any number of Domain Controllers can be added.
4. Data Collection will happen only for the Number of Domain Controller licenses purchased. The rest of the Domain controllers will be in a Disabled State.

For purchasing the license or any queries, please contact sales@manageengine.com. The license file will be sent through e-mail.

To upgrade from a Trial Edition or Free Edition to Standard Edition

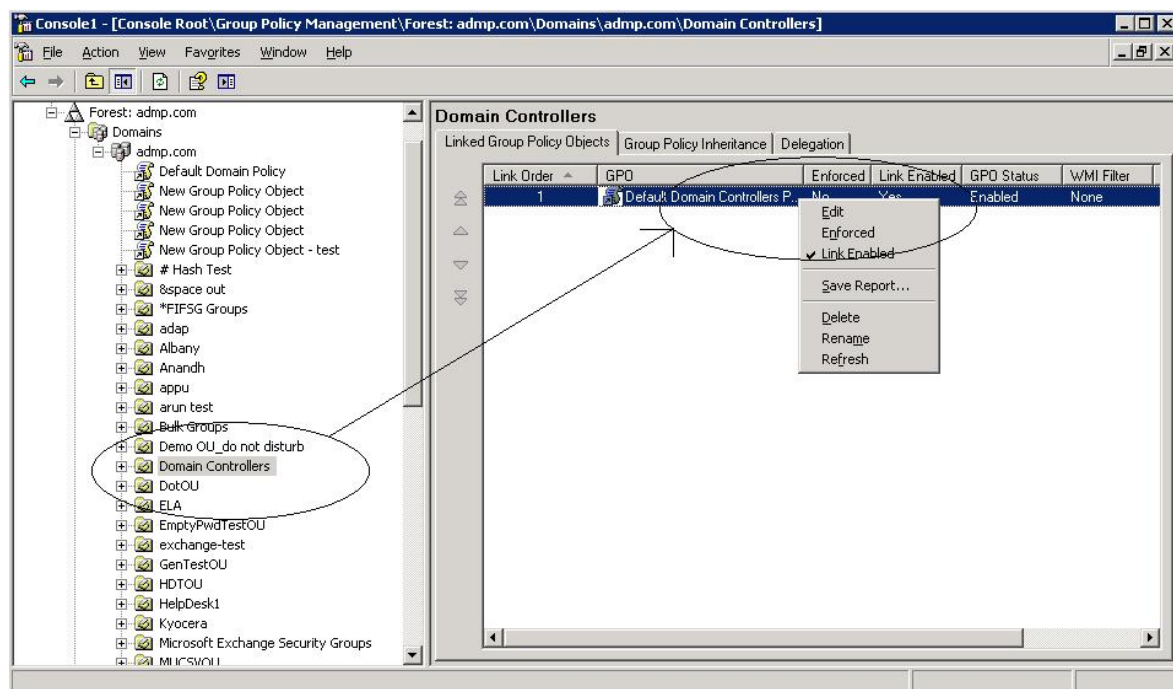
1. Click the License link available in the top right corner of the ADAudit Plus client. This opens the License details of the product.
2. Click the Upgrade Now link and select the license file received from AdventNet using the Browse button.
3. Click Upgrade button to upgrade from Trial or Free Edition to Professional Edition.

Configuring Audit Policy Settings

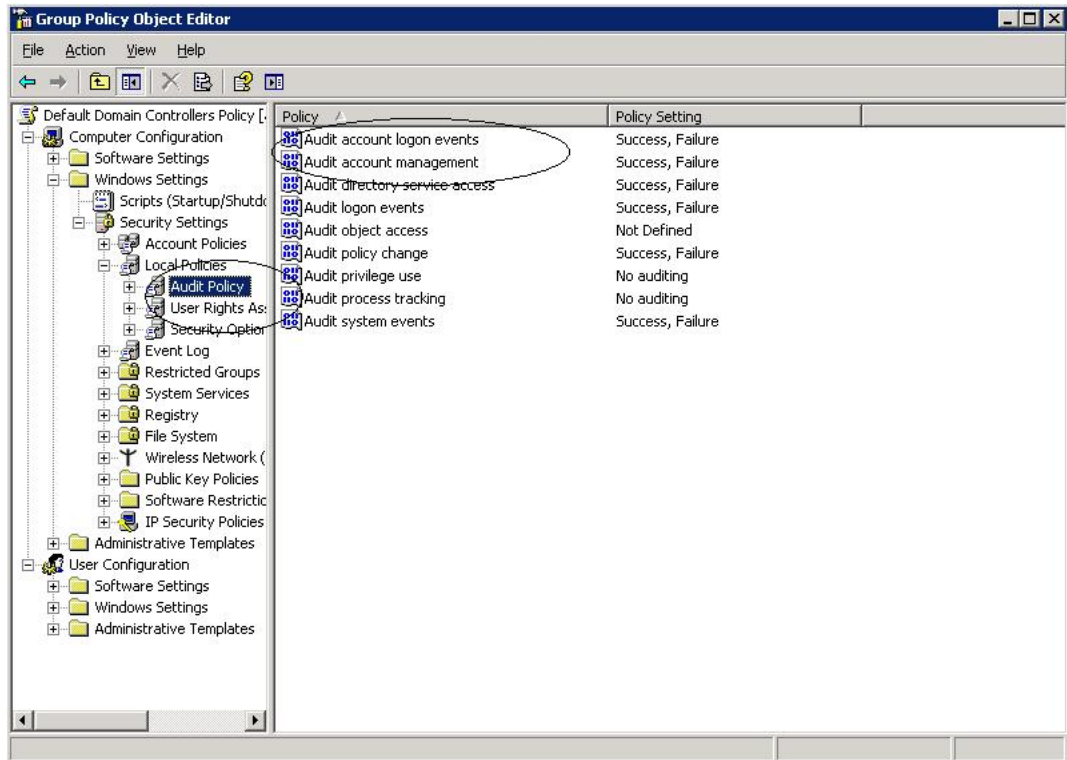
NOTE: To audit domain logon activities and account management activities, you must use the Group Policy snap-in to enable the Audit "Account Logon" and "Account Management" settings in the Audit Policy.

To enable local Windows security auditing:

1. Log on to Windows with an account that has Administrator rights.
2. Ensure that the Group Policy snap-in is installed.
3. **Open the GPMC (Group Policy Management Console) in Windows 2003 servers.**



4. Navigate to "Default Domain Controller's Policy"(GPMC -> Domain Controllers Container -> Default Domain Controllers Policy)
5. Click on "Edit".
6. Navigate to "Audit Policy" node, "Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy"
7. From the right pane, double-click the policy that you want to configure (enable/disable). This will bring up the 'Audit system events properties' dialog.
8. Configure "Audit account logon events", both "Success" and "Failure".
9. Similarly configure "Audit account management".
10. For GPO and OU Auditing. Ensure that the Directory Service Access Success auditing in the Default Domain Controllers Policy is enabled.



This policy setting will be replicated across all Domain Controllers which enable auditing of the corresponding activities.

Configuring SACLs for GPO and OU Objects

To allow ADAudit Plus to report on Security events - the System Access Control Lists (SACL) must be set accordingly in your Auditing Policy settings of the ADUC ("Active Directory Users and Computers" console) on your Domain Controller machine.

To perform this procedure, you must be a member of the "Domain Admins group" or the "Enterprise Admins group" in Active Directory, or you must have been delegated the appropriate authority. As a security best practice, consider using Run as to perform this procedure.

In this page we will discuss:

1. Steps to access the ADUC console from the Start Menu
2. Steps to enable Advanced Security settings for the Domain.(Fig1)
 1. Organizational Unit Audit entries to be enabled in the Advanced configuration settings of the Domain. ADAudit Plus provides reports only those OU entries configured. (Table1)
 2. Group Policy object Audit entries to be enabled in the Advanced configuration settings of the Domain. ADAudit Plus provides reports only those GPO entries configured. (Table2)
3. Advanced security auditing entries - enabled for Domain OU and GPO objects – (Fig3).

1. Steps to access the ADUC console from the Start Menu

1. Open "**Active Directory Users and Computers**".
 1. (Click "**Start**" --> Click "**Control Panel**" --> double-click "**Administrative Tools**" and then -->> double-click "**Active Directory Users and Computers** ")

2. Steps to enable Advanced Security settings for the Domain.(Fig2)

1. Ensure that View --> "**Advanced Features**" are selected from the drop down. This will display the Advanced Security settings for selected objects in the Active Directory Users and Computers.
2. In the console tree, right-click the "**domain**"
3. Click "Properties", and then click the "**Security**" tab.
4. Click "**Advanced**" to open the Window to enter "Advanced Security Settings for the Domain"
5. Click "**Add**" to add the security principal you want to apply the security policy (In our case it is "**Everyone**") and click on **OK**
6. This opens the window to select "Permission Entries for the Domain"

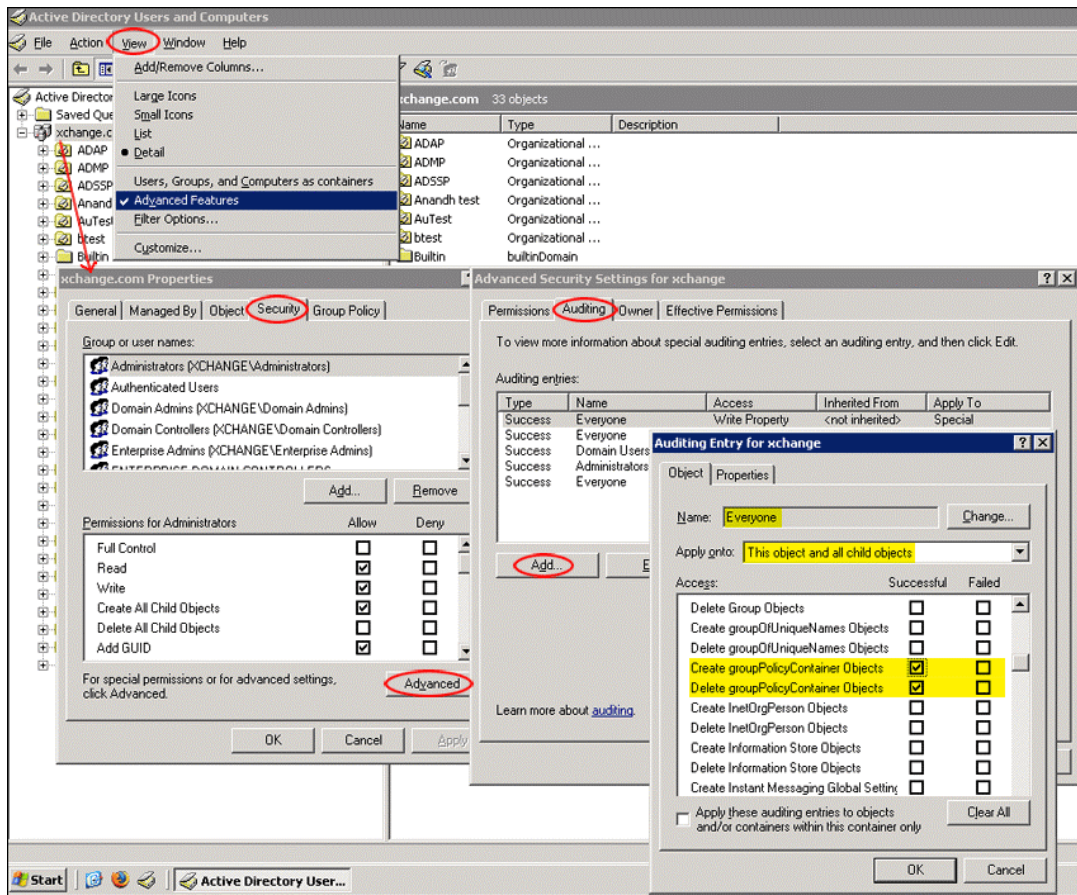


Fig2: Selecting the Advanced security setting for a domain

1. Enable the below Auditing Entries for Organizational Units

	Object to set SACL on	Auditing entries to be applied on	Type	Access	Apply onto
SACLs to Create, Delete OU object	Domain	Everyone	Successful	Create organizationalUnit Object, Delete organizationalUnit Object	This object and all child objects
SACLs to Write All Properties, Delete, and Modify Permissions for Organizational Unit objects	Domain	Everyone	Successful	Write All Properties, Delete, Modify Permissions	Organizational Unit objects
SACLs to enable auditing Child Objects(Users, Groups, Computers) Creation in OU	Domain	Everyone	Successful	Create user Object, Create group Object, Create computer Object	This object and all child objects

2. Enable Audit Entries for groupPolicy objects

	Object to set SACL on	Auditing entries to be applied for	Type	Access	Apply onto
SACLs to Create, Delete Group Policy Objects	Domain	Everyone	Successful	<ul style="list-style-type: none"> Create groupPolicyContainer Objects Delete groupPolicyContainer Objects 	This object and all child objects
SACLs to Write All Properties, Delete, and Modify Permissions for groupPolicyContainer objects	Domain	Everyone	Successful	<ul style="list-style-type: none"> Write All Properties Delete Modify Permissions 	groupPolicyContainer objects

3. Advanced Security auditing entries - enabled for the Domain OU and GPO objects

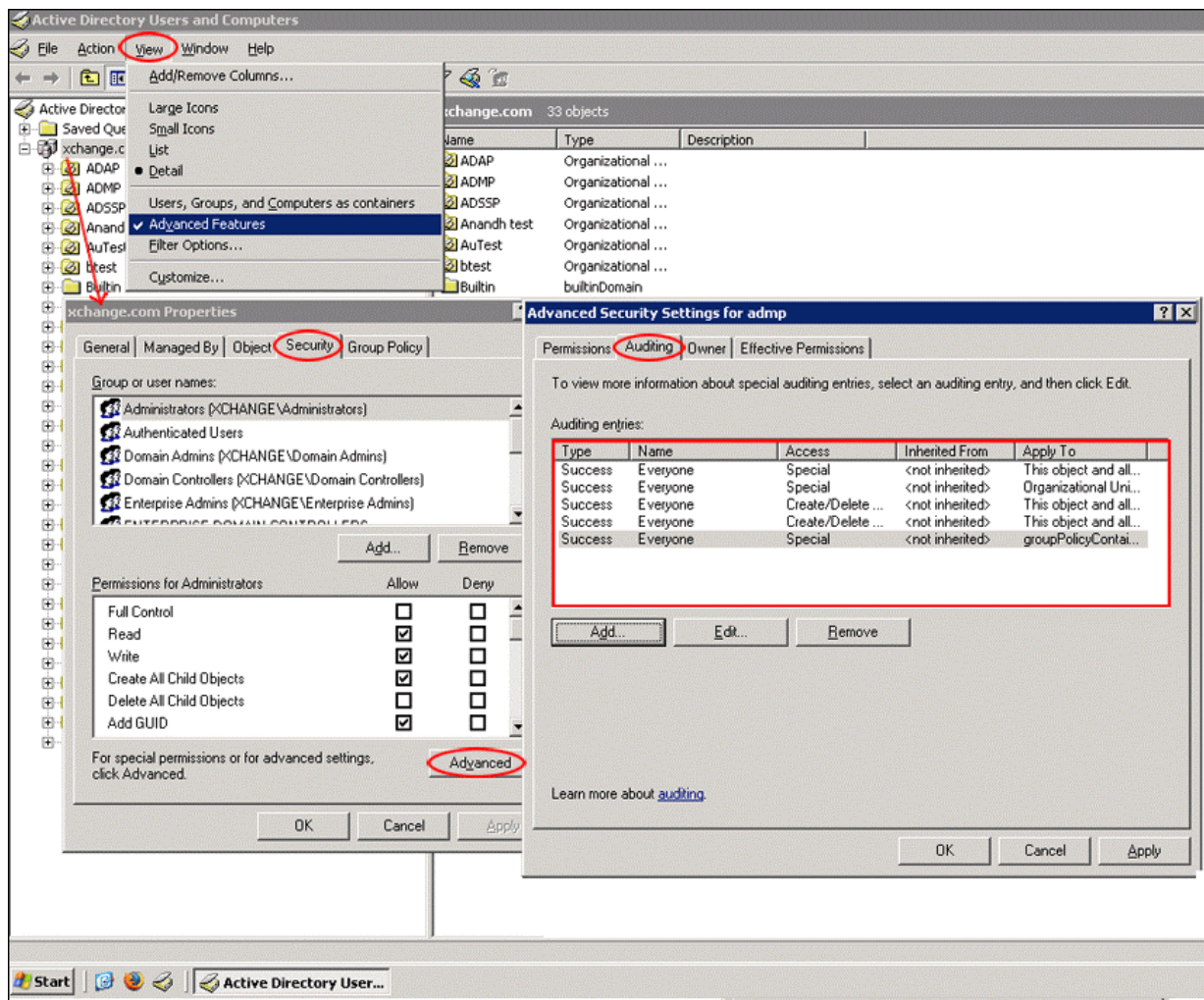


Fig3: Advanced Security setting for Organizational Unit and Group Policy Objects

Dashboard View

The Home Tab which is the default Dashboard for ADAudit Plus provides a quick snapshot of essential audit data. Audit data of all configured Domains can be viewed from an intuitive graphic display. The graphic display helps in easier understanding of information from the dashboard view itself.

Further The display information is grouped by Domains and Desired / Undesired Audit activities like

- Logon Failures,
- User Creation,
- Logon Failure -Error Code
- Logon Peak hour usage
- Account locked out users
- Password Changed Users

are displayed on the dashboard by default.

- A 7 day or 30 day snapshot from the graphic display makes it easier for an administrator to identify when a desired / undesired audit event has occurred.
- Trend lines for 7 day and 30 days helps easier understanding the trends over a period of time.
- Administrators can click on the graphics to view its underlying data.

Reports


ADAudit Plus has a plethora of reports to audit your Active Directory efficiently from anywhere in the domain. An audit entry in the Security log contains the following information:

- The action that was performed.
- The user who performed the action.
- The success or failure of the event and the time that the event occurred.

ADAudit Plus reports can be accessed by selecting the Reports tab from the client window they are grouped under the following categories by default.

1. User Logon Reports
2. User Management Reports
3. Group Management Reports
4. Computer Management Reports
5. GPO Management Audit Reports
6. OU Management Audit Reports
7. Domain Policy Changes Reports
8. Profile Based Reports

These reports can be scheduled and also emailed to one or more email ids. More on Schedule Reports discussed under the Schedule Reports section.

	<p>GPO Audit and OU Audit are done for the SACLs enabled or selected to be audited. Security Access Control Limitations are set in the ADUC (Active Directory Users and Computers) under the Advanced properties tab.</p> <ul style="list-style-type: none"> • To enable audit entries for GPO Management Audit follow the below steps. • To enable audit entries for OU Management Audit follow the below steps.
---	---

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.
- 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.
- Perform a quick search by inputting any attribute value that is displayed in the columns.
- 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. More on Schedule Reports.

User Logon Reports

This reporting module provides audit information on user logon. ADAudit Plus has a list of pre-configured reports to extract audit information on User Logon and is readily available for the user on installing the product.

Pre-configured Audit Reports for User Logon Include:

- Logon Failures
- Domain Controller Logon Activity
- Member Server Logon Activity
- Workstation Logon Activity
- User Logon Activity
- Recent User Logon Activity
- Last Logon on Workstations

Logon Failure Report:

Logon failure is an error case which prevents a user from Logging into the Domain.

A Logon Failure can occur as a result of any one of the below provided reasons.

- Bad User Name
- New computer account has not replicated yet or computer is pre-w2k
- Administrator should reset the password on the account
- Workstation/Logon time restriction
- Account disabled, expired, or locked out
- Password has expired
- Bad password
- Time in workstation is not in sync with the time in Domain Controllers

To view an Audit Report on Logon Failure

1. Click on the 'Reports' Tab --> User Logon Reports --> Logon Failure
2. Select the Domain
3. Select the Period (Period between 1 hr and 23 hours) A custom period can also be selected.
4. This Lists the audit information on 'Logon Failure' for the selected period.
5. A graphic display for easier viewing of status is also provided.

Attributes related to Logon Failure audit which include { User Name, Client Machine Name, Domain Controller, Logon Time, Event Type, Failure Reason, Host Name, Remarks, Event Number, Failure Type, Domain, Logon Service, SID, Event Code } can be added or removed to the 'Logon Failure' Audit Report using the Add/ Remove Columns link.

Domain Controller Logon Activity:

To View an Audit Report on Domain Controller Logon Activity

1. Click on the 'Reports' Tab -->> User Logon Reports -->> Domain Controller Logon Activity
2. Select the 'Domain'
3. Select the 'Domain Controller'
4. This lists the audit information of Domain Controller Logon Activity for the selected "Domain Controller".
5. A Bar Graph with the "Hour of Logon Activity" on the X axis and "Logon Count" on the Y axis is provided to help in viewing the Trend of Domain Controller Logon Activity at any given hour of a day from the date of configuration for a selected Domain Controller.(This helps to identify **peak logon times** for any selected Domain Controller).
6. The Bar Graph facilitates "Filtering" the report for a selected Hour.
7. Quick search option can be used for granular filter

Attributes related to Domain Controller Logon Activity Audit include {User Name, Client Machine Name, Domain Controller, Logon Time, Event Type, Failure Reason, Host Name, Remarks, Domain, Logon Service, Failure Type, SID, Event Number, Event Code } can be added or removed as desired.

Member Server Logon Activity:

To View an Audit Report on "Member Server Logon Activity "

1. Click on the 'Reports' Tab -->> User Logon Reports -->> Member Server Logon Activity
2. Select the 'Domain' from the Drop Down.
3. Click the 'Server' link to Select the "Server" (Use the Quick Find from the Pop Up if you know the name of the 'Server'.)
4. This lists the audit information of Member Server Logon Activity for the selected "Server".
5. The details of users who have logged on to the Member Server is displayed on a "Pie Chart".
6. Select an area of the "Pie Chart" to view the details of the selected user.
7. Quick search option can be used for granular filter from the report against its columns.

One or all of the Available Attributes listed here {User Name,Client IP Address,Client Host Name,Domain Controller,Logon Time, Event Type, Failure Reason, Remarks, Domain, Logon Service,Failure Type, SID,Event Number, Event Code } can be added to the columns for Audit of "Member Server Logon Activity".

Workstation Logon Activity:

This report provides information on the Logon activity done on a selected Workstation.

To View an Audit Report on "Workstation Logon Activity".

1. Click on the 'Reports' Tab -->> User Logon Reports -->> Workstation Logon Activity
2. Select the Domain from the Drop Down.
3. Click the 'Select' link to Select the "Computer" (Use the Quick Find from the Pop Up if you know the name of the 'Computer' or Workstation.)
4. This lists the audit information on Logon Activity done on the selected "Workstation or Computer".
5. The details of users who have logged on to the Member Server is displayed on a "Pie Chart".

6. Select an area of the "Pie Chart" to view the details of the selected "Computer" or "Workstation".
7. Quick search option can be used for granular filter from the report against its columns.

One or all of the Available Attributes listed here { User Name, Client IP Address, Client Host Name, Domain Controller, Logon Time, Event Type, Failure Reason, Remarks, Domain, Logon Service, SID, Event Number, Event Code, Failure Type } can be added to the columns for Audit of Workstation Logon Activity.

User Logon Activity

This report provides audit information on all Logon activities done by a selected user.

To View an Audit Report for User Logon Activity

1. Click on the 'Reports' Tab -->> User Logon Reports -->> User Logon Activity
2. Select the Domain from the Drop Down.
3. Click the 'Select' link to Select the "User" (Use the Quick Find from the Pop Up if you know the name of the 'User'.)
4. This lists the audit information of User Logon Activity for the selected "User".
5. The details of the selected User Logon Times and the total count at an hour of a day is displayed with the help of a bar graph.(The Bar Graph helps to identify **Peak Logon Time of Day** for any selected user in the selected Domain).
6. Click on any "Hour of Day" from the Graph to view a list of all the Dates and Times of Logon for the selected user.
7. Quick search option can be used for granular filter from the report against its columns.

Audit Information of a User Logon Activity which include User Name, Client IP Address, Client Host Name, Domain Controller, Logon Time, Event Type, Failure Reason, Remarks, Domain, Logon Service, Failure Type, SID , Event Number, Event Code are all listed for a selected user under a single report. An administrator can Add / Remove one or more of these selected columns and view a report desired or needed.

Recent User Logon Activity

This Report provides Audit Information on all success / failure attempts made by users to Logon for the time selected. Recent Logon Activity Report by default provides Logon Activity of all users in the Recent 24 Hours. However a Custom Period can also be selected.

To View an Audit Report on Recent User Logon Activity

1. Click on the 'Reports' Tab -->> User Logon Reports -->> Recent User Logon Activity
2. Select the Domain from the Drop Down.
3. Select the Period from the Drop Down. (The period ranges from 1 hour to 24 hours with options to select Today, Yesterday and also a Custom Period.).
4. The list of all users who have recently logged on is displayed in the report.
5. The status of Logon Activity (Success / Failure) is highlighted with a Pie Chart.
6. Select the area of the "Pie Chart" to view the details on (Success / Failure) of Logon Activity details for the selected period.

Audit Information of a Recent User Logon Activity can include one or more of the below columns.

{User Name, Client IP Address, Client Host Name, Domain Controller, Logon Time, Event Type, Failure Reason, Remarks, Domain, Logon Service, Failure Type, SID, Event Number, Event Code }

Last Logon on Workstations

This report lists information on the time of last logon on to a Workstation or Computer, by all the users who have successfully logged on.

To View a Report on Last Logon on Workstation

1. Click on the 'Reports' Tab --> User Logon Reports --> Last Logon on Workstation
2. Select the Domain from the Drop Down.
3. This lists the Client Host Name / Client IP Address of the Workstation and the details of user who has made a last Logon on the Client.
4. The Last Logon Time and the Domain Controller for the Logon Activity are listed by default.

Other attributes can be added/ removed from Add /Remove Attributes link provided.

User Management

This reporting module lists audit information on all user management actions.

- Recently Created Users
- Recently Deleted Users
- Recently Enabled Users
- Recently Disabled Users
- Recently Locked Out Users
- Recently Unlocked Users
- Recently Password Changed Users
- Recently Password Set Users
- Recently Modified Users
- Last Modification on Users
- User Activity
- User History

Recently Created Users

This Report Provides Audit Information on all Recently created Users. User Created (Account Name / Sam Account Name), Who created the user (Caller User Name) , When was the user created (Creation Time), and others.

To view an Audit Report on Recently Created Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Created Users
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Users Created' in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the users created by him.

One or all of the Available Attributes can be added to the columns to be monitored for Users Created.

Recently Deleted Users

This Report Provides Audit Information on all Recently deleted Users. User Created (Account Name / Sam Account Name), Who created the user (Caller User Name) , When was the user created (Deletion Time), and others.

To view an Audit Report on Recently Deleted Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Deleted Users
2. Select the 'Domain' from the drop down.

3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the "Users Deleted" in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the users deleted by him.

One or all of the Available Attributes listed here {User Name Caller User Name Deleted Time Domain Controller Remarks Caller Logon ID Domain Caller User Domain Modification Type SID Event Number Event Type Event Code } can be added to the columns to be monitored.

Recently Enabled Users

This Report provides Audit Information on Recently enabled users. The list of users enabled in the selected time period, the "Caller User" ie) who enabled them, the times at which the users were enabled can be viewed.

To view an Audit Report on Recently Enabled Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Enabled Users
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the "Users Enabled" in the selected period.
5. A Pie Chart displays the split up of the "Caller user" who modified the users.

Other attributes of Audit can be added or removed using the Add / Remove column link.

Recently Disabled Users

This Report provides Audit Information on Recently Disabled users.

To view an Audit Report on Recently Disabled Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Disabled Users
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the "Users Disabled" in the selected period.
5. A Pie Chart displays the split up of the "Caller user" who modified the users.

Other attributes of Audit can be added or removed using the Add / Remove column link.

Recently Locked Out Users

This Report provides Audit Information on Recently Locked Out Users. The User who was locked out, the times at which the user was Locked Out in the selected period, and the Caller Machine Name during Account Lockout.

To view an Audit Report on Recently Locked Out Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Locked Out Users
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the "Users Locked Out" in the selected period.
5. A Pie Chart displays the split up of the "Caller user" who modified the users.

Other attributes of Audit can be added or removed using the Add / Remove column link.

Recently Unlocked Users

This Report provides Audit information on all the users whose accounts have been unlocked in the selected period. Information like User Name, the Caller User Name, the time of unlock (modified time), Event Type (Success / Failure) and other audit information can be monitored.

To view an Audit Report on Recently Unlocked Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Unlocked Users
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected from the drop down).
4. This Lists the audit information on all the "User Accounts Unlocked" in the selected period.
5. A Pie Chart displays the split up of the "Caller user" who Unlocked the users.

Other attributes of Audit can be added or removed using the Add / Remove column link.

Recently Password Changed Users

This report provides audit information on Users whose Passwords were Changed in the selected period of time. Information like User Name, the Caller User Name, the time of Password Change (Modified Time), Event Type (Success / Failure) and other audit information can be monitored.

To view an Audit Report on Recently Password Changed Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Password Changed Users
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected from the drop down).
4. This Lists the audit information on all the "Recently Password Changed User Accounts" for the selected period.
5. A Pie Chart displays the split up of the "Caller user" who Changed the Password of the Accounts.

Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Password Set Users

This report provides audit information on Users whose Passwords were set in the selected period of time. Information like User Name, the Caller User Name, the time Password was set Change (Modified Time), Event Type (Success / Failure) and other audit information can be monitored.

To view an Audit Report on Recently Password Set Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Password Set Users
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected from the drop down).
4. This Lists the audit information on all the "Recently Password Set User Accounts" for the selected period.
5. A Pie Chart displays the split up of the "Caller user" who Set the Password of the User Accounts.

Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Modified Users

This report provides Audit Information on the Users who were modified in the selected period of time. Information like User Name, the Caller User Name, Modified Time, Modified Attributes and the Domain Controller are displayed.

To view an Audit Report on Recently Modified Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Modified Users
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected from the drop down).
4. This Lists the audit information on all the "Recently Modified User Accounts" for the selected period.
5. A Pie Chart displays the split up of the "Caller user" who Modified the User Accounts.

Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Last Modification on Users

This report lists audit information on the Last Modification Activity done on Users Accounts. The user, the caller name and the attribute modified are displayed.

To view a report Last Modification on Users

1. Click on the 'Reports' Tab -->> User Management -->> Recently Modified Users
2. Select the 'Domain' from the drop down.
3. This list the audit information on Last Modification on Users with the Message Example :
User account 'User Name' was changed by 'Caller User Name'. Changed Attributes :
'Modified Attribute' the Modified Time is also displayed for all the users.

Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

User Activity

This report provides audit information on all account management activities done by a selected user. The Report is Grouped under User Management, Computer Management and Group Management.

To view the complete User Activity done on other users

1. Click on the 'Reports' Tab -->> User Management -->> User Activity
2. Select the 'Domain' from the drop down.
3. Select the User for whom activities done should be monitored. (Click select -->>select user -->>click on OK)
4. To View "User Management" actions done click on "User Management" Tab
5. This lists all the User Management actions done by the user.
6. To View "Computer Management" actions done by the selected user click on "Computer Management" Tab.
7. This lists all the Computer Management actions done by the user.
8. To View "Group Management" actions done by the selected user click on ""Group Management" Tab.
9. This lists all the Group Management actions done by the user.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

User History

This report provides audit information on Active Directory User Object's History. The Caller User Names of who modified the Selected User Object and when (Modified Times).

To view the complete audit information on the activities done on a selected user.

1. Click on the 'Reports Tab' -->> User Management --> User History
2. Select the Domain from the Drop Down
3. Select the "User" whose history is to be monitored. (Click select -->>select user -->>click on OK)
4. This lists the audit information on all activities done on the selected user.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Group Management

This reporting module lists audit information on all Group management actions.

- Recently Created Security Groups
- Recently Created Distribution Groups
- Recently Deleted Security Groups
- Recently Deleted Distribution 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 History

Recently Created Security Groups

This Report Provides Audit Information on all Recently Created Security Groups.

To view an Audit Report on Recently Created Security Groups

1. Click on the 'Reports' Tab -->> Group Management -->> Recently Created Security Groups
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Security Groups Created in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the Security Groups created by him.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Created Distribution Groups

This Report Provides Audit Information on all Recently Created Distribution Groups.

To view an Audit Report on Recently Created Distribution Groups

1. Click on the 'Reports' Tab -->> Group Management -->> Recently Created Security Groups
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Distribution Groups Created in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the Security Groups created by him.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Deleted Security Groups

This Report Provides Audit Information on all Recently Deleted Security Groups.

To view an Audit Report on Recently Deleted Security Groups

1. Click on the 'Reports' Tab -->> Group Management -->> Recently Deleted Security Groups
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Security Groups Deleted in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the Security Groups created by him.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Deleted Distribution Groups

This Report Provides Audit Information on all Recently Deleted Distribution Groups.

To view an Audit Report on Recently Deleted Distribution Groups

1. Click on the 'Reports' Tab -->> Group Management -->> Recently Deleted Distribution Groups
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Distribution Groups Deleted in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the Distribution Groups Deleted by him.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Added Members to Security Groups

This Report Provides Recently Added Members to Security Groups.

To view an Audit Report on Recently Added Members to Security Groups

1. Click on the 'Reports' Tab -->> Group Management -->> Recently Added Members to Security Groups
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Recently Added Members to Security Groups in the selected period.
5. A Pie Chart displays the split up of the "Caller users" and the Recently Added Members to Security Groups by the caller users.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Added Members to Distribution Groups

This Report Provides audit information on Recently Added Members to Distribution Groups.

To view an Audit Report on Recently Added Members to Security Groups

1. Click on the 'Reports' Tab -->> Group Management -->> Recently Added Members to Distribution Groups
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Recently Added Members to Distribution Groups in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the Recently Added Members to Distribution Groups by the Caller User.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Removed Members from Security Groups

This Report Provides audit information on Recently Removed Members from Security Groups.

To view an Audit Report on Recently Removed Members from Security Groups

1. Click on the 'Reports' Tab -->> Group Management -->> Recently Removed Members from Security Groups
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Recently Removed Members from Security Groups in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the Recently Removed Members from Security Groups by each Caller User.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Recently Removed Members from Distribution Groups

This Report Provides audit information on Recently Removed Members from Distribution Groups.

To view an Audit Report on Recently Removed Members from Distribution Groups

1. Click on the 'Reports' Tab -->> Group Management -->> Recently Removed Members from Distribution Groups
2. Select the 'Domain' from the drop down.

3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Recently Removed Members from Security Groups in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the Recently Removed Members from Distribution Groups by each Caller User.

To view audit details on any specific activity click on the Pie Chart or Use the Quick Search option. Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Group History

This Report Provides audit information on an Active Directory Group Object's History. The Caller User Names of who modified the Selected Group Object and when (Modified Times).

To view Group History in a selected domain.

1. Click on the 'Reports' Tab -->> Group Management -->> Group History
2. Select the 'Domain' from the drop down.
3. Select the Group. (Click on Select link -->>Select Group -->> Click OK)
4. This Lists the Group History for the Selected Group.

Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Computer Management

This reporting module lists audit information on all Computer management actions.

- Recently Created Computers
- Recently Deleted Computers
- Recently Modified Computers
- Recently Enabled Computers
- Recently Disabled Computers
- Computer History

Recently Created Computers

This report provides audit information on all recently created computers. Who created the computers (Caller User Name), Name of Computers Created.

To view a report on Recently Created Computers

1. Click on the 'Reports' Tab -->> Computer Management -->> Recently Created Computers
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Computers Created' in the selected period.
5. A Pie Chart displays the split up of the "Caller users" and the Computers created by them.

To view other audit attributes click on Add Remove Columns link and select the attributes from the list of available attributes.

Recently Deleted Computers

This report provides audit information on all recently deleted computers. Who deleted the computers (Caller User Name), Name of Computers Deleted.

To view a report on Recently Deleted Computers

1. Click on the 'Reports' Tab -->> Computer Management -->> Recently Deleted Computers
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Computers Deleted' in the selected period.
5. A Pie Chart displays the split up of the "Caller users" and the Computers deleted by them.

To view other audit attributes click on Add Remove Columns link and select the attributes from the list of available attributes.

Recently Modified Computers

This report provides audit information on all recently deleted computers. Who modified the computers (Caller User Name), Name of Computers modified.

To view a report on Recently Modified Computers

1. Click on the 'Reports' Tab -->> Computer Management -->> Recently Modified Computers
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Computers Created' in the selected period.
5. A Pie Chart displays the split up of the "Caller users" and the Computers modified by them.

To view other audit attributes click on Add Remove Columns link and select the attributes from the list of available attributes. The Remarks column provides info on what modification action was done.

Recently Enabled Computers

This report provides audit information on all recently enabled computers. Who modified the computers (Caller User Name), Name of Computers enabled in the selected period for the selected domain and the exact time a computer was enabled.

To view a report on Recently Modified Computers

1. Click on the 'Reports' Tab -->> Computer Management -->> Recently Enabled Computers
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Computers Enabled in the selected period.
5. A Pie Chart displays the split up of the "Caller users" and the Computers enabled by them.

To view other audit attributes click on Add Remove Columns link and select the attributes from the list of available attributes.

Recently Disabled Computers

This report provides audit information on all recently disabled computers. Who modified the computers (Caller User Name), Name of Computers disabled in the selected period, for the selected domain and the exact time a computer was disabled.

To view a report on Recently Modified Computers

1. Click on the 'Reports' Tab -->> Computer Management -->> Recently Disabled Computers
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period can also be selected).
4. This Lists the audit information on all the Computers Disabled in the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the Computers disabled by him.

To view other audit attributes click on Add Remove Columns link and select the attributes from the list of available attributes.

Computer History

This Report Provides audit information on Computer History for any selected Computer in a Domain.

To view the History of any Computer in a selected domain.

1. Click on the 'Reports' Tab -->> Computer Management -->> Computer History
2. Select the 'Domain' from the drop down.
3. Select the Computer. (Click on Select link -->>Select Group -->> Click OK)
4. This Lists the History of the selected Computer.

Other attributes of Audit can be added or removed using the "Add / Remove Columns" link.

Group Policy Objects (GPO) Management Audit Reports

This reporting module provides audit information on all organizational unit changes for one or multiple selected Group Policy objects. The GPO Management reports can also be scheduled to run at user defined times and also be emailed to user mailboxes on a hourly, daily, weekly or monthly intervals.

Pre-configured Audit Reports for GPO Management Audit Include:

- Recently Created GPOs
- Recently Deleted GPOs
- Recently Modified GPOs
- GPO Link Changes
- GPO History

Recently Created GPOs:

The Recently Created GPOs report of ADAudit Plus lists all Group Policy Objects created within a given span of time. Change information like who created the GPO, the time it was created, From where was the GPO created are listed in a single report and displayed on the ADAudit Plus user interface. A pie chart provides information on all GPOs and is split to provide information on users who created them.

To view an Audit Report on Recently Created GPOs click on the link **Recently Created GPOs** available under the GPO Management category and follow the below steps.

1. Select the 'Domain' from the drop down.
2. Select the Period (Today, Yesterday, This Week, This Month or any custom period) from the drop down.
3. This Lists the audit information on all the 'GPOs Created' for the selected period.

One or all of the Available Attributes can be added to the columns to be monitored for GPOs Created. A Pie chart highlights all users who created GPOs. Clicking a user from the Pie chart displays the complete information about that GPOs deleted by that user.

Recently Deleted GPOs:

The Recently Deleted GPOs report of ADAudit Plus lists all Group Policy Objects deleted within a given span of time for a selected domain. Change information like who deleted the GPO, the time it was deleted, From where was the GPO deleted are listed in a single report and displayed on the ADAudit Plus user interface.

To view an Audit Report on Recently Deleted GPOs click on the link **Recently Deleted GPOs** available under the GPO Management category.

A Pie chart highlights all users who modified GPOs. Clicking a user from the Pie chart displays the complete information about that GPOs deleted by that user.

Recently Modified GPOs:

The Recently Modified GPOs report of ADAudit Plus lists all Group Policy Objects modified. Change information like who modified the GPO, the time it was modified, From where was the modification done are listed in a single report and displayed on the ADAudit Plus user interface. By default, the report displays the GPOs modified in the last 30 days week. You have an option to choose a different period or to generate a report for a custom period.

To view an Audit Report on Recently Modified GPOs click on the link **Recently Modified GPOs** available under the GPO Management category.

A Pie chart highlights all users who modified GPOs. Clicking a user from the Pie chart displays the complete information about that GPOs modified by that user.




GPO Link Changes:

Provides the list of GPOs that are linked to OUs in the domain. To view the report, click the **GPO Link Changes** link available under the GPO Management Reports category. Clicking a GPO from the report displays the complete information about that GPO Link Changes.

GPO History:

The "GPO History" Report lists the detailed history of changes that have occurred on any selected Group Policy Object. GPO history of a single or multiple GPOs in a selected domain can be viewed on a single web interface.

To view an Audit Report on GPO History:

1. Click on the 'Reports' Tab --> GPO Management --> GPO History
2. Select the 'Domain' from the drop down.
3. To select one or multiple GPOs for which the History is to be reported. click on the Add  Button.
4. To remove one or multiple GPOs whose GPOs History need not be reported. Click on the GPO link -->From the Popup Select GPOs to be removed and click  Remove
5. Select the Period (Today, Yesterday, This Week, This Month or any custom period) from the drop down.
6. This Lists the audit history of all the GPOs for the selected period.
7. To view the audit history of any specific GPOs use the Filter  option by selecting the GPO.
8. A Pie Chart displays the split up of the "History of Actions" that occurred on the selected GPOs. Click on any action to view filtered information on who did the selected actions.

Organizational Units Management Audit Reports

Organizational Units (OUs), are administrative-level containers on a computer network that allow network administrators to organize groups of users together, so that any changes or any other administrative tasks could be accomplished more efficiently. Using "OU" administrator can group objects into logical units and also place users, groups, computers, and other organizational units.

This reporting module provides audit information on all organizational unit changes for one or multiple selected OUs. The OU Management reports can also be scheduled to run at user defined times and also be emailed to user mailboxes on a hourly, daily, weekly or monthly intervals.

Pre-configured Audit Reports for OU Management Audit Include:

- Recently Created OUs
- Recently Deleted OUs
- Recently Modified OUs
- OU History

Recently Created OUs:

The Recently Created OU report of ADAudit Plus lists all Organizational Units created within a given span of time. Change information like who created the OU, the time it was created, From where was the OU created are listed in a single report and displayed on the ADAudit Plus user interface. A pie chart provides information on all OUs and is split to provide information on users who created them.

Click on any user highlighted in the chart to view the list of OUs created by him for the selected time period.

To view an Audit Report on Recently Created OUs

1. Click on the 'Reports' Tab -->> OU Management -->> Recently Created OUs
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period) from the drop down.
4. This Lists the audit information on all the 'OUs Created' for the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the OUs created by the user.

One or all of the Available Attributes can be added to the columns to be monitored for OUs Created.

Recently Deleted OUs:

The Recently Deleted OUs report of ADAudit Plus lists all Organizational Units deleted within a given span of time for a selected domain. Change information like who deleted the OU, the time it was deleted, From where was the OU deleted are listed in a single report and displayed on the ADAudit Plus user interface. A pie chart provides information on all OUs and is split to provide information on users who deleted them.

Click on any user highlighted in the chart to view the list of OUs deleted by him for the selected time period.

To view an Audit Report on Recently Deleted OUs

1. Click on the 'Reports' Tab -->> OU Management -->> Recently Deleted OUs
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period) from the drop down.

4. This Lists the audit information on all the 'OUs Deleted' for the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the OUs deleted by the user.

One or all of the Available Attributes can be added to the columns to be monitored for OUs Deleted.

Recently Modified OUs:

The Recently Modified OU report of ADAudit Plus lists all Organizational Units modified within a given span of time. Change information like who modified the OU, the time it was modified, From where was the modification done are listed in a single report and displayed on the ADAudit Plus user interface. A pie chart provides information on all OUs and is split to provide information on users who modified them.

OU Modifications captured and reported by ADAudit Plus include : changes to OU properties, changes to OU permissions, renaming of the OU and any object/objects added to the OU.

Click on any user highlighted in the chart to view the list of OUs modified by him for the selected time period.

To view an Audit Report on Recently Modified OUs



1. Click on the 'Reports' Tab -->> OU Management -->> Recently Modified OUs
2. Select the 'Domain' from the drop down.
3. Select the Period (Today, Yesterday, This Week, This Month or any custom period) from the drop down.
4. This Lists the audit information on all the 'OUs Modified' for the selected period.
5. A Pie Chart displays the split up of the "Caller user" and the OUs modified by the user.

One or all of the Available Attributes can be added to the columns to be monitored for OUs Modified.

OU History:

The "OU History" Report lists the detailed history of changes that have occurred on any selected Organizational Unit. OU history of a single OU or multiple OUs in a selected domain can be viewed on a single web interface.

To view an Audit Report on OU History:

1. Click on the 'Reports' Tab -->> OU Management -->> OU History
2. Select the 'Domain' from the drop down.
3. To select one or multiple OUs for which the History is to be reported. click on the Add  Button.
4. To remove one or multiple OUs whose OUs History need not be reported. Click on the OU link -->From the Popup Select OUs to be removed and click  Remove
5. Select the Period (Today, Yesterday, This Week, This Month or any custom period) from the drop down.
6. This Lists the audit history of all the OUs for the selected period.
7. To view the audit history of any specific OUs use the Filter option by selecting the OU.
8. A Pie Chart displays the split up of the "History of Actions" that occurred on the selected OUs. Click on any action to view filtered information on who did the selected actions.

Domain Policy Changes

- Domain Policy Changes

Domain Policy Changes

This Report provides audit information on policy changes done in any selected domain. Policy "Lockout Policy Changes" and "Password Policy Changes" can be monitored from the report. The report provides audit information on what attribute was modified, modified time, and who modified the attribute.

To View a report of Domain Policy Changes

1. Click on Reports -->> Domain Policy Changes -->> Domain Policy Changes
2. Select the Domain from the Drop Down
3. This list all the Policy Changes done in the selected domain
4. A Pie Chart provides a split up of the Caller Users who made policy changes in the selected domain.

Use the Add /Remove columns option to view a specific attribute to be monitored. The quick search option can be used to get filtered results.

Profile Based Reports

Profile Based Reports is an important feature of ADAudit Plus. This allows a user to create his own desired report profiles. The report profiles are configured using the configuration Tab in ADAudit Plus. Any number of Report Profiles can be configured.

Default Profile Based Reports

ADAudit Plus provides pre-configured audit reports under the below mentioned categories.

1. Account Logon
2. Account Creation
3. User Modification
4. Computer Modification
5. Group Modification
6. Domain Policy Changes
7. GPO Management Changes
8. OU Management Changes

To view more on advanced configuration and default reports available click [here](#).

Account Logon Category

Pre-Configured Actions for Account Logon in ADAudit Plus

- Logon Failure Events
- Logon Success Events

Account Creation Category

Pre-Configured Actions for Account Creation in ADAudit Plus

- Security Group created
- Distribution Group created
- User Account Created
- Computer Account created

User Modification Category

Pre-Configured Actions for User Modification in ADAudit Plus

- User Account was Locked
- User Account was Unlocked
- User Password was set
- User Account Enabled
- User Account Disabled
- User Password was changed
- User Name Changed
- User Account Modified
- User Account Deleted

Computer Modification Category

Pre-Configured Actions for Computer Modification in ADAudit Plus

- Computer account Modified
- Computer Name Changed
- Computer account deleted
- Computer account disabled
- Computer account enabled

Group Modification Category

Pre-Configured Actions for Group Modification in ADAudit Plus

- Distribution group deleted
- Member Added to Security Group
- Group Name Changed
- Member Removed from Security Group
- Member Removed from Distribution Group
- Security Group Deleted
- Member added to Distribution group

Domain Policy Changes Category

Pre-Configured Actions for "Domain Policy Changes Category" in ADAudit Plus

- Domain Policy Changed

GPO Management Changes

Pre-configured reports on GPO change actions provided in ADAudit Plus.

- GPO Created
- GPO Deleted
- GPO Modified
- GPO Link Changes
- GPO Permission Changed

OU Management Changes

Pre-configured reports on OU change actions provided in ADAudit Plus

- OU Created
- OU Deleted
- OU Renamed
- OU Permission Changed
- OU Modified
- Child Objects Created in OU
- OU Moved

Schedule Reports

Once a report is created, schedules can be set up in ADAudit Plus to run the selected reports automatically at specified time intervals. ADAudit Plus can also be configured to automatically email the report once it runs at desired time intervals.

The reports scheduled to run are generated and stored at a user defined storage path. These reports and can be e-mailed as a compressed zip file, a link or as an attachment in any of the listed formats - pdf, xls, csv or html.

To Schedule a New Report

- Click on the "Admin" Tab -->> "Schedule Reports" under Administration -->> "Schedule New Reports"
- Enter the "Schedule Name" and the "Description" for the schedule in the respective Text boxes.
- Select the "Domain Name" from the Drop Down.

Attribute	Description
Schedule Name	Enter a unique name to identify this schedule
Description	Enter a description corresponding to the schedule name.
Domain Name	Select the Domain Name from the drop down. The Drop Down lists all configured Domain names.

Scheduler Creation

Once the schedule name, its description and the domain where the schedule is to be run is defined, the actual schedule creation needs to be done. The Scheduler Creation section of ADAudit Plus discusses about.





Select Reports	Select one or more "Available Reports" to be scheduled under the given "Schedule Name". Both default and User defined Reports can be added to the "Selected Reports" by clicking on the "Add>>" link.
Schedule Report Frequency	The "Selected Reports" can be scheduled on a 'Hourly', 'Daily', 'Weekly' or 'Monthly' basis. The report is scheduled to run once for the frequency selected.
Schedule Report Format	The Scheduled Reports can be stored in 'pdf', 'xls', 'html', or 'csv' formats. They are stored at the "File Storage Path" entered by click on the "File Storage Path" link.
Email Notification	The scheduled report can be e-mailed to any email-id entered in the "specify email address" box on providing a check against "Email this scheduled report".

Select Reports

ADAudit Plus allows you to select one or more reports to be run at scheduled times. The selection of all reports that are to be scheduled is done here. Both user defined and default reports can be selected from the list of available reports by click on the "Add" link against the respective reports.

On clicking the "Add" link, the reports under the "Available Reports" column are selected and moved to the "Selected Reports" column.

On clicking the "Remove" link, the reports selected and listed under the "Selected Reports" column are unselected and moved to the "Available Reports" column.

	<ul style="list-style-type: none"> • Move your cursor on the "Available Reports" table and click on the icon  to select user(s), on the icon  to select computer(s) or on the icon  to select group(s). The icons are displayed only against the reports that require granular object selection. • The objects selected can also be removed by using the "more" link of the "Selected Reports" table.
---	--

Schedule Report Frequency

Different schedules will require different frequencies to be selected and this is facilitated here. ADAudit Plus allows to select the below frequencies.

The schedule can be selected for daily, weekly or hourly by selecting the respective radio buttons.

Frequency	Description
Hourly	If you want to schedule this report to run every hour, enter the time after which this report has to run every one hour.
Daily	If you want to schedule this report to run every day, enter the time at which this report has to run every day. With data being fetched 24 hours from time of schedule (or) The previous day (0:00 hours to 23:59 hours)
Weekly	If you want to schedule this report to run every week, enter the date and time at which this report has to run every week. With data being fetched 7 days from day of schedule (or) The previous week (Monday to Sunday).
Monthly	If you want to schedule this report to run every month, enter the day and time at which this report has to run every month. With data being fetched 30 days from day of schedule (or) The previous month (Day 1 to Day 30).

Provided below are the steps to schedule an hourly report

"Selected Reports" or the "Schedule" will be scheduled to run once every hour.

To set the frequency of the schedule to "Hourly".

- Select the "Hourly" Radio option under "Schedule Report Frequency"
- Enter the Starting time for the Schedule. This schedule will be run on a Hourly basis from the start time selected.

<ul style="list-style-type: none"> • Previous Hour - When a user selects the "Last Hour" option from the drop down. The data will be fetched once every time the clock ticks a valid hour. Eg. (9:00 O' Clock, 10:00 O' clock etc.,) • Last 60 minutes - This depends on the start time selected. The data will be fetched exactly 1 hour (60 minutes) from the time selected as start time.
--


Schedule Report Format

The Scheduled Reports can be stored in 'pdf', 'xls', 'html', or 'csv' formats by selecting the format of choice from the drop down.

They are stored at the "File Storage Path" entered by click on the "File Storage Path" link.

1. The default "File Storage Path" is ' %Product Home Folder%\webapps\adap\schedule-reports\ '. The user can change the storage path for the scheduled reports to any desired location.
2. The "File Server Path" is ' \\file-server\share-folder\ '

3. Outside the product it is 'D:\ADAudit Plus\schedule-reports\ '

	<p>If you modify the default "File storage path", scheduled reports cannot be viewed through the web console.</p>
---	---

Email Notification

The scheduled report can be sent to any email-id entered in the text box "specify email address" on providing a check against "Email this scheduled report".

Email Notification requires

1. Configuring the "Message Settings"
2. Emailing the Scheduled Report

Message Settings

The "Message Settings" needs to be configured to define the text message and the format (link or attachment) in which the scheduled report will be delivered to a users email id.

To configure the "Message Settings"

- Click on the "Message Settings" link under Email Notification
- Select the options of your choice from the pop-up menu that is displayed.
- Enter the Mail content Entering the " Subject" and "Message" in their respective boxes provided.
- Click on OK.

Options selected to email or publish a scheduled report:

Email Reports as an attachment	Reports are emailed as an attachment. The format of choice is selected under "Schedule Report Format" and could be any of the slected formats pdf, csv, html or xls .
Email Reports as a Zip File	The selected reports are compressed to a zip format and emailed.
Publish the report and email the link alone	Selecting this option the reports are published and the published link alone is emailed to users.

Emailing a Scheduled Report:

To notify a scheduled report by email:

- Provide a check against "Email this scheduled report" under Email Notification section.
- Specify email address in the Text box that is displayed.
- Click on save.

This will email the scheduled report in the desired format (selected under "message settings") to all entered email addresses.

Alerts

ADAudit Plus facilitates an easy to understand alerting mechanism to alert on any configured change event. The alerts are based on the event data obtained from a configured Report Profile.

- Alert in Audit Plus
- Configuring an Alert
- Manage Alerts by clearing or deleting them
- Notify Alerts by Email

An Alert in ADAudit Plus

Alerts in ADAudit Plus enables real time monitoring of a change in the Active Directory. An alert will include the following information,

- Source
- Domain
- Severity
- Alert Message
- Time Generated.

Source :

This is the Domain Controller from which Event Originated.

Domain :

This provides the Domain Information.

Severity :

Severity indicates the degree of importance associated with an event. ADAudit Plus provides 3 different alert notifications which include

1. Attention
2. Trouble
3. Critical

The degree of importance or the Severity to be associated with an event is decided and configured by an administrator while configuring Alert Profiles.

Alert Message :

Details of the generated alert provided in a easy-to-understand format.

Example: Login failure for User 'Administrator' in '192.168.117.56'. Reason: 'Bad password'

Time Generated:

This is the time when the Alert was generated.

Configure / Create Alert Profiles:


ADAudit Plus facilitates an administrator to create customized Alert Profiles by associating them to a Report Profile of choice. To configure / create an alert profile click [here](#).

Manage Alerts

ADAudit Plus allows an administrator to manage his alerts by clearing or deleting them with the **Clear / Delete** alerts options.


To Clear an Alert

1. Click on the "Alerts" Tab (This displays alerts in the configured Domain Controllers)
2. Select "Active Alerts" from the Drop down (This displays only the Active Alerts in the Configured Domain Controllers)
3. Select the Alerts to be cleared by providing a check against the respective Alerts.
4. Click on 'Clear' (This will clear the selected alerts)

	<p>Notes:</p> <ol style="list-style-type: none"> 1. Only real time alerts which are unattended/uncleared are visible under the "Active Alerts" Table. 2. Once an alert is attended it can be cleared. 3. Cleared alerts will be visible under the "All Alerts" Table.
---	--

To Delete an Alert

1. Click on the "Alerts" Tab (This displays alerts under the configured the Domain Controllers)
2. Select "Active Alerts" from the Drop down (This displays only the Active Alerts in the Configured Domain Controllers)
3. Select the Alerts to be cleared by providing a check against the box provided against them.
4. Click on 'Delete' (This will delete the selected alerts)

	<p>Notes:</p> <ol style="list-style-type: none"> 1. Clearing or Deleting of Alerts is possible for both "Active Alert" or "All Alert" options selected from the drop down. 2. An Alert once deleted will not be visible under any of the Alert Tables. 3. Cleared alerts along with real time alerts will be visible under the "All Alerts" Table. 4. "Report Profile Based Alerts" or "Alert Profile Based Alerts" can be viewed and managed by selecting respective Alert Tables.
---	---

Notify Alerts by Email

An important part of an alert is its ability to notify users. Alerts configured in ADAudit Plus can be notified to one or more recipients by email.

To configure an email alert from the "Alert" Tab

1. Click on the "Email Notification" Link to the top right of the page.
2. This will redirect to the "Configuration" Tab showing all "Available alert profiles".
3. Click on the "Configure" link under the column "E-mail Notify".
4. This will redirect to the page where you can "Modify Alert Profiles"

5. Under "Modify Alert Profile" provide a check against "Send E-mail Notification".
6. Enter the "Mail To" address in the check box provided. (For multiple recipients, separate email addresses with commas.)
7. Click on "Update".

This will update the "Alert Profile" for the "Selected Report Profile". Any new alert will be notified by email to one or all email addresses entered here. This is also discussed under the Alert Profiles Configuration Section.



The "Mail To" Box will be open for entry only if a Mail Server is configured. To configure mail Server click on the "Configure Mail Server" Link.

Configuration

Configuration Tab in ADAudit Plus allows an administrator to configure

1. Report Profiles
2. Alert Profiles
3. Audit Actions and
4. Advanced Configuration.

Report Profiles

A Report Profile exhibits an association of filtered event data. The filtered event data in the Report Profile consists of Active Directory user, computer, group objects and their association with audit actions.

- Configuring Report Profiles
- Report Profile Categories
- Selecting Objects for Association

Configuring Report Profiles

To configure a Report Profile an administrator can select any of the available report profile categories, map them with an action and associate this with Domain Object / Objects.

A report profile will include

1. A report profile name
2. Category under which the report profile is mapped.
3. Actions - Actions depend on the Category Selected. To know more about Actions click [here](#).
4. Associated Domain Objects - Domain Objects like Users, Groups, or Computers can be associated

Steps to Configure a Report Profile:

1. Click on Configuration Tab -->> New Report Profile
2. Name the Report Profile in the Box Provided.
3. Provide a Description of the Report Profile in the Box Provided.
4. Select a Category from the Drop Down.
5. Select "Actions"
6. All Actions corresponding to the "Report Profile Category" Selected are displayed.
7. Provide a check against one or all the Actions that needed to be displayed in the configured report.
8. This Maps Actions for a selected Report Profile Category.
9. Select the Domain (From the Drop Down)
10. Select the Users / Computers / Groups (This is based on the "Report Profile Category")
11. Click on Save.
12. This associates the Domain Objects to Mapped "Report Profile Category".
13. A Report Profile with the "Report Profile Name" inputted is configured.
14. The Report Profile Created is also added under the Reports Tab.(Profile Based Reports under the respective domain.



Note: Any Number of Actions can be configured / added in a selected category. To add / configure new actions for a selected category used the [Advanced Configurations](#) Option



Note: The Report Profile created is added under "Configuration" Tab -->>"Report Profile Categories" -->>"Available Report Profiles".
Click on View Reports link to view a report for any Configured Report Profile.

Report Profile Categories

Report Profile Categories in ADAudit Plus include:

- Account Logon
- Account Creation
- User Modification
- Computer Modification
- Group Modification
- Domain Policy Changes

Selecting Objects for Association:


Objects will include Users, Computers, Groups or the entire Domain.

- Selecting Users for Association
- Selecting Computers for Association
- Selecting Groups for Association
- Selecting a Domain for Association

Selecting Users for Association:

Account Logon / User Creation and User Modification Report Profile Categories, require a user to be associated.


To select one or multiple users

1. Click the filter icon 
2. Provide a check against the users.
3. Multiple Users can also be selected by Groups, or OU's using the link available in the Pop-Up.
4. Users in the Entire Domain can also be selected by providing a Check against the Domain.

Selecting Computers for Association:

Computer Creation / Computer Modification Report Profile Categories will need a computer to be associated.


To select one or multiple computers:

1. One or Multiple Computers can be selected from the Pop-Up on clicking the filter icon 
2. Provide a check against the Computers.
3. Multiple Computers can also be selected by **Groups**, or **OU's** using the link available in the Pop-Up.
4. Computers in the Entire Domain can also be selected by providing a Check against the Domain.

Selecting Groups for Association

Group Creation / Group Modification Report Profile Categories will need a group to be associated.

To select one or multiple Groups:

1. One or Multiple Groups can be selected from the Pop-Up on clicking the filter icon 

2. Providing a check against the users.
3. Multiple Groups can also be selected **OU's** using the link available in the Pop-Up.
4. Groups in the Entire Domain can also be selected by providing a Check against the Domain.

Selecting a Domain for Association:

Domain Policy Changes Report Profile Categories need to facilitate a Domain to be associated.

A domain can be directly selected from the drop down when a "Domain Policy change" Report Profile Category is selected.

Alert Profiles

- Create Alert Profile
- View / Modify Alert Profiles
- Notify Alerts by Email

Create Alert Profile

The below mentioned requirements are to be met for an Alert Profile.

1. Name of the Alert Profile
2. Description for the Alert Profile
3. Severity of the Alert configured.
4. Report Profiles to be Associated with the Alert Profile.
5. Alert Message.

To create a New Alert Profile:

1. Click on "Configuration" Tab -->>"Create Alert Profile" under Alert Profiles.
2. This displays the Create Alert Profile Page.
3. Enter the "Name" of the Alert Profile in the Box Provided.
4. Enter the "Description" of the Alert Profile in the Box Provided.
5. Select the "Severity" of the Alert Profile
 - The Severity depends on importance of the Alert and can indicate "Attention, Trouble, or Critical"
6. 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.
7. 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".
8. 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.
9. Click on "Save"
10. A new Alert Profile is created.

View / Modify Alert Profiles

Viewing an Alert Profile

To view all alert profiles in ADAudit Plus

1. Click on "Configuration" Tab -->>"View / Modify Alert Profiles" under Alert Profiles.
2. This lists all available Alert Profiles in ADAudit Plus.
3. Information on when a Report Profile was created and when last modified is displayed for All Report Profiles.


Modifying an Alert Profile

An existing Alert Profile can be modified by changing one or all of the below

1. Modifying the Name of the Alert Profile
2. Modifying the Description for the Alert Profile
3. Modifying the Severity of the Alert configured.
4. Modifying the Report Profiles
5. Modifying the Alert Message.
6. Notify Alerts by Email


Modifying the Name of the Alert Profile

To modify the name of an Alert Profile.

1. Click on "Configuration" Tab -->>"View / Modify Alert Profiles" under Alert Profiles.
2. This lists all available Alert Profiles in ADAudit Plus.
3. To modify any of the Available Alert Profile click on the modify icon  against the Alert Profile to be modified.
4. Modify the existing "Name" in the Name Box Provided.
5. Click on Update.
6. This updates the Name of the Alert Profile to the newly named Alert Profile.


Modifying the Description for the Alert Profile

To Modify the Description for the Alert Profile

1. Click on "Configuration" Tab -->>"View / Modify Alert Profiles" under Alert Profiles.
2. This lists all available Alert Profiles in ADAudit Plus.
3. To modify any of the Available Alert Profile click on the modify icon  against the Alert Profile to be modified.
4. Modify the existing "Description for the Alert Profile" in the Description Name Box Provided.
5. Click on Update.
6. This updates the Description for the Alert Profile.



Modifying the Severity of the Alert configured.

To Modify the Severity of the Alert configured:

1. Click on "Configuration" Tab -->"View / Modify Alert Profiles" under Alert Profiles.
2. This lists all available Alert Profiles in ADAudit Plus.
3. To modify any of the Available Alert Profile click on the modify icon  against the Alert Profile to be modified.
4. To Modify the "Severity" select from the Drop Down between "Trouble, Attention and Critical".
5. Click on Update.
6. This updates the Severity Profile for any selected Report Profile.


Modifying the Report Profiles

To Modify the Report Profiles

1. Click on "Configuration" Tab -->"View / Modify Alert Profiles" under Alert Profiles.
2. This lists all available Alert Profiles in ADAudit Plus.
3. To modify any of the Available Alert Profile click on the modify icon  against the Alert Profile to be modified.
4. To Modify the "Report Profile" for a Domain
 - On Clicking the  Plus icon 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.
 - "Profile Based Reports" which are configured in ADAudit Plus by an User can also be added and alerted.
 - Click on OK.
 - The Report Profiles are now associated with the Alert.
5. Click on Update.
6. This updates the "Report Profile Based Alerts" under the Alerts Tab of ADAudit Plus and also under their corresponding Domains.

Modifying the Alert Message

To Modify the Alert Message Displayed for an Alert

1. Click on "Configuration" Tab -->"View / Modify Alert Profiles" under Alert Profiles.
2. This lists all available Alert Profiles in ADAudit Plus.
3. To modify any of the Available Alert Profile click on the modify icon  against the Alert Profile to be modified.
4. To Modify the 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 messages can also be configured.
 - To configure a Customized Message

- Add Text using the Add Text Box -->>click on Add
 - Add Variable selecting from the Drop Down and click on Add.
 - Confirm the message from the "Alert Message Box"
 - Click on OK.
5. Click on Update.
 6. This updates the Alert Message against the "Alert Message" column under the Alerts Tab.

Notify Alerts by Email

An important part of an alert is its ability to notify users. ADAudit Plus facilitates notifications of one or all configured Alerts by email.

To configure an email alert directly from the Alert Tab

1. Click on the "Email Notification" Link to the top right of the page.
2. This will redirect to the "Configuration" Page showing all "Available alert profiles".
3. Click on the "Configure" link under the column "**E-mail Notify**".
4. This will redirect to the page where you can "Modify Alert Profiles"
5. Under "Modify Alert Profile" provide a check against "Send E-mail Notification".
6. Enter the "Mail To" address in the check box provided. (For multiple recipients, separate email addresses with commas.)
7. Click on Update.

This will update the "Alert Profile" for the "Selected Report Profile". Any new alert will be notified by email to one or all recipient email addresses entered here.



The Mail To Box will be open only when Mail Server is configured. To configure mail Server click on the "Configure Mail Server" Link.

Audit Actions

Default Audit Actions in Audit Plus include the below listed types grouped under various categories.

- Account Logon
- Account Creation
- User Modification
- Computer Modification
- Group Policy Objects (GPO) Changes
- Organizational Units (OU) Management Changes
- Group Modification
- Domain Policy Changes

The Advanced Configuration option allows to include custom defined Actions

Advanced Configurations

Advanced Configurations in ADAudit Plus allows a user to define one or more audit actions that needs to be reported. It facilitates filtering rules for a user to create new actions or modify any of the pre-configured actions. Filters help to define actions to suit his reporting need.

Default Audit Actions and Configuring New Actions

ADAudit Plus has a list of pre-configured Audit Actions which are associated with their respective report profile categories. Pre-Configured Audit Actions provided by ADAudit Plus are provided after a detailed study on commonly used auditing actions in various environments. To know more on the Pre-Configured Actions for Report Profile Categories, Steps to create a New Action for Report Profile Category, Copying and Modifying an Action.



- Account Logon
- Account Creation
- User Modification
- Computer Modification
- Group Modification
- Domain Policy Changes
- Group Policy Objects (GPO) Management Changes
- Organizational Unit (OU) Management Changes

Account Logon Category

Pre-Configured Actions for Account Logon in ADAudit Plus


- Logon Failure Events
- Logon Success Events
- Logon Failure Events 2000 AD

To configure a New Account Logon Action:



1. Click on Configuration --> Advanced Configuration .
2. Click on "New Account Logon Action".
3. Enter the "Action Name".
4. Enter the "Description" for Action Name.
5. Enter the "Rule Group Name".
6. Create "Filter Rules".
7. A Filter Rule is a combination of a Variable and a Value connected by a relational operator.
8. The Variable and the Relational Operator can be selected from Drop Downs.
9. Variables listed in the Drop Down correspond to Account Logon.
10. Any Number of filter rules can be added to a Rule Group.
11. To add a Filter Rule, click on the Plus Icon .
12. To remove Filter Rule, click on the cross icon .

13. A Rule Group is defined by one or more filter rules combined by a common logical operator (**AND** or **OR**).
14. Any Number of Rule Groups can be Added.
15. Click on "Add Rule Group" button to add a New Rule Group.
16. To delete a Rule Group use the "Delete Rule Group" Button.
17. Click on Update to Save the configured Action with the Action Name Provided.

To Modify an Account Logon Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on Modify Icon  against the Account Logon Action that needs to be modified.
3. This allows to modify the Account Logon Action for the Action Selected.

To Copy an Account Logon Action

1. Click on Configuration -->> Advanced Configuration .
2. Click on Copy Icon  against the Account Logon Action that needs to be copied.
3. A copy of the Action Selected is created with a Name "Copy of ***** ".
4. To modify the copy Click on Modify Icon 

Account Creation Category


Pre-Configured Actions for Account Creation in ADAudit Plus

- Security Group created
- Distribution Group created
- User Account Created
- Computer Account created


To configure a New Account Creation Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on "New Account Creation Action".
3. Follow the steps as for Account Logon Action.

To Modify an Account Creation Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on Modify Icon  against the Account Creation Action that needs to be modified.
3. This allows to modify the Account Creation Action for the Action Selected.

To Copy an Account Creation Action

1. Click on Configuration -->> Advanced Configuration .
2. Click on Copy Icon  against the Account Creation Action that needs to be copied.
3. A copy of the Action Selected is created with a Name "Copy of ***** ".

4. To modify the copy Click on Modify Icon 
-

User Modification Category


Pre-Configured Actions for User Modification in ADAudit Plus

- User Account was Locked
- User Account was Unlocked
- User Password was set
- User Account Enabled
- User Account Disabled
- User Password was changed
- User Name Changed
- User Account Modified
- User Account Deleted



To configure a New User Modification Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on "New Account Creation Action".
3. Follow the steps as for Account Logon Action.

To Modify an User Modification Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on Modify Icon  against the User Modification Action that needs to be modified.
3. This allows to modify the User Modification Action for the Action Selected.

To Copy an User Modification Action

1. Click on Configuration -->> Advanced Configuration .
 2. Click on Copy Icon  against the "User Modification Action" that needs to be copied.
 3. A copy of the Action Selected is created with a Name "Copy of ***** ".
 4. To modify the copy Click on Modify Icon 
-

Computer Modification Category


Pre-Configured Actions for Computer Modification in ADAudit Plus

- Computer account Modified
- Computer Name Changed
- Computer account deleted
- Computer account disabled
- Computer account enabled



To configure a New Computer Modification Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on "New Computer Modification Action".
3. Follow the steps as for Account Logon Action.

To Modify an Computer Modification Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on Modify Icon  against the Computer Modification Action that needs to be modified.
3. This allows to modify the Computer Modification Action for the Action Selected.

To Copy a Computer Modification Action

1. Click on Configuration -->> Advanced Configuration .
2. Click on Copy Icon  against the "Computer Modification Action" that needs to be copied.
3. A copy of the Action Selected is created with a Name "Copy of ***** ".
4. To modify the copy Click on Modify Icon 

Group Modification Category


Pre-Configured Actions for Group Modification in ADAudit Plus

- Distribution group deleted
- Member Added to Security Group
- Group Name Changed
- Member Removed from Security Group
- Member Removed from Distribution Group
- Security Group Deleted
- Member added to Distribution group



To configure a New Group Modification Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on "New Computer Modification Action".
3. Follow the steps as for Account Logon Action.

To Modify a Group Modification Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on Modify Icon  against the Computer Modification Action that needs to be modified.
3. This allows to modify the Computer Modification Action for the Action Selected.

To Copy a Group Modification Action

1. Click on Configuration -->> Advanced Configuration .
 2. Click on Copy Icon  against the "Group Modification Action" that needs to be copied.
 3. A copy of the Action Selected is created with a Name "Copy of ***** ".
 4. To modify the copy Click on Modify Icon 
-

Domain Policy Changes Category


Pre-Configured Actions for "Domain Policy Changes Category" in ADAudit Plus

- Domain Policy Changed



To configure a New Domain Policy Change Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on "New Domain Policy Changes Action".
3. Follow the steps as for Account Logon Action.

To Modify a Domain Policy Change Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on Modify Icon  against the Domain Policy Changes Action that needs to be modified.
3. This allows to modify the Domain Policy Changes Action for the Action Selected.

To Copy a Domain Policy Change Action

1. Click on Configuration -->> Advanced Configuration .
 2. Click on Copy Icon  against the "Domain Policy Changes Action" that needs to be copied.
 3. A copy of the Action Selected is created with a Name "Copy of ***** ".
 4. To modify the copy Click on Modify Icon 
-

Group Policy Object (GPO) Management Category

Before extracting the reports ensure that the below audit entries are enabled in the SACL (Security Access Control Limits for the Domain). Click here to view SACLS to enabled for GPOs.


Pre-configured reports for "GPO Management" category in ADAudit Plus.

- GPOs Created
- GPOs Deleted
- GPOs Modified
- GPO Link changes



To configure a New GPO Management Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on "New GPO Management Action".
3. Follow the steps as for Account Logon Action.

To Modify a GPO Management Change Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on Modify Icon  against the "GPO Management Action" that needs to be modified.
3. This allows to modify the "GPO Management Action" for the Action Selected.

To Copy a GPO Management Change Action

1. Click on Configuration -->> Advanced Configuration .
2. Click on Copy Icon  against the "GPO Management Action" that needs to be copied.
3. A copy of the Action Selected is created with a Name "Copy of ***** ".
4. To modify the copy Click on Modify Icon 

Organizational Unit (OU) Management Category

Before extracting the OU change reports ensure that the below audit entries for OUs are enabled in the SACL (Security Access Control Limits for the Domain). Click here to view SACLS to enabled for GPOs.


Pre-configured reports for "OU Management" category in ADAudit Plus.

- OUs Created
- OUs Deleted
- OUs Modified



To configure a New OU Management Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on "New OU Management Action".
3. Follow the steps as for Account Logon Action.

To Modify a OU Management Change Action:

1. Click on Configuration -->> Advanced Configuration .
2. Click on Modify Icon  against the "OU Management Action" that needs to be modified.
3. This allows to modify the "OU Management Action" for the Action Selected.

To Copy a OU Management Change Action

1. Click on Configuration -->> Advanced Configuration .
2. Click on Copy Icon  against the "OU Management Action" that needs to be copied.
3. A copy of the Action Selected is created with a Name "Copy of ***** ".
4. To modify the copy Click on Modify Icon 

Admin

The Admin Tab in ADAudit Plus talks about

- General Settings
- Domain Settings

General Settings

The General Settings for ADAudit Plus include.

- Personalize Settings
- Connection Settings
- Server Settings
- Mail Server Settings

The above mentioned topic provide general information on the settings to be made in ADAudit Plus.

Personalize

ADAudit Plus provides users with the functionality to configure user accounts based on personal priorities and requirements. The Personalize option enables you to change an existing password and a user interface theme.

To change the password

1. Enter the existing password in the **Old Password** field.
2. Enter the new password in the **New Password** field.
3. Enter the new password again for confirmation in the **Confirm Password** field.
4. Click the **Save Changes** button.

The new password gets updated. Subsequently, you have to use the new password to login to the client.

To change the theme

1. Select the theme from the available options
2. Click **Save Changes** button.

Connection

You can Change the connection settings using this option. To change the connection settings perform the following steps

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

Server

You can Configure ADAudit Plus at startup & also set the log settings from here.

1. Select the **Admin** tab.
2. Click on **Server**.
3. Check one or all the Boxes you wish.
 1. Start the product automatically on Windows Startup [Applicable for service installation. Start-->All programs-->ADAudit Plus-->NT Service -->Install ADAP Service]
 2. Launch the ADAudit Plus client upon successful startup
4. The default working mode for ADAudit Plus is 'Normal' with minimal set of debugging information.
5. click on 'Save changes' .
6. This configures the **Server Settings** for ADAudit Plus.

Mail Server Settings

The mail server settings are configured in-order to send alert email notifications.

Configuring Mail Server Settings

1. Click on "Admin" Tab -->> "Mail Server Settings" (Under General Settings)
2. Specify the "Mail Server" and "Mail Port" in the respective boxes provided.
3. Check against the "Authentication" and enter 'Username' and 'Password' of the Mail Server to avoid anonymous login.
4. In the "From" Address field enter the e-mail address from which you are likely to receive the report mails.
5. Click on "Save Changes".

Your mail server has been configured.

To verify your mail server settings you can send a test email from the "Send Test Mail" Link. A test email will be delivered to the "recipient email addresses" entered here from the configured Mail Server.

Administration

ADAudit Plus allows ease of administration of various Domain components and also helps in managing notifications and archives.

Administration deals with

- Domain Settings
- Alerts
- Archive Settings
- Schedule Reports
- Event CleanUp
- Technician Settings

Domain Settings

The Domain Settings link is present at the top right corner of ADAudit Plus. This link helps to configure Domains, Domain Controllers and also facilitates enabling / disabling a Domain or Domain Controller. More on Configuring Domains and Domain Controllers is discussed below.

- Configuring Domains and Domain Controllers
- Schedule Domain Controllers to fetch event data

Configuring Domains and Domain Controllers

- Actions performed on a Domain
- Actions performed on a Domain Controllers

During startup, ADAudit Plus adds all the domains that could be discovered. If you wish to add more domains or modify the added domains, you can do it from here.

To add more domains, follow the steps below:

1. Click the **Domain Settings** link from the client to open the Domain Settings page.(This is present at the Top Right corner of ADAudit Plus)
2. The domains that are already added are listed here. Click the add new domain link to open the **Add Domain Details** dialog.
3. Specify the Domain Name.
4. Click on **Discover** link to locate the domain controllers from the DNS and add. Else, add all the domain controllers manually. The domain controller that appears first in the list is considered as the primary domain controller. Use the up and down arrows to move the added domain controllers in the order of priority.
5. To **ADD Multiple Domain Controllers**, input the domain controllers separated by a comma (,) sign.
6. Specify the authentication details of the user as which the domain controller will be contacted.
7. Click **ADD** to add the domain.








Note: The procedure to add domains like Child Domains, Domains from same and different forests are the same.








Note: Domain Controllers can also be added from the link "Add Domain Controllers" at the bottom of each Domain Details.

You can perform the following actions from here on a Domain:

1. **Default Domain:** The domain that is first discovered is considered as default domain. If you wish to change the default domain, click the icon  from the action column to make it default .
2. **Modifying Domain:** To modify the domain details, click the modify  icon and change the required values and save.

3. **Deleting a Domain:** To delete a domain, click the delete  icon.
4. **Refreshing the Domain Details:** To synchronize the object details with the Active Directory, click the  icon.

You can perform the following actions from here on a Domain Controller:

1. Any number of Domain Controllers can be added to fetch event data based on the license purchased.
2. In the **Trial Edition** only 5 Domain controllers can be configured to collect data.
3. Though more domain controllers can be added / discovered, only 5 domain controllers will be enabled  to fetch audit data the rest will be disabled .
4. An administrator can **enable**  or **disable**  a Domain Controller to fetch event data by providing a check against the icon provided.
5. To **delete** a Domain Controller click on the Delete Icon .



Note: In the Free Edition fresh event data is not fetched. But data fetched during the last trial / licensing period is reported.

Configure Domain Controllers to fetch event data:

Event Data can be fetched from all the Domain controllers that are configured under domains which have proper privileges. To designate proper privileges one needs to enter proper credentials while configuring domains.

1. ADAudit Plus lists all available Domain Controllers in an organized format. Domain Controllers are listed under their corresponding Domains.
2. Event Update Runs once every 2 Hours for each Domain Controller by default. ADAudit Plus can be configured to change the Event Update schedule to run between 1 and 23 Hours by click on the change **link** and selecting the Time duration from the Drop Down.
3. ADAudit Plus provides details on **Last Event Read Time**.
4. To facilitate latest event data to be fetched from a selected Domain Controller a **[Run Now]** option is also available.
5. The Status column provides information on whether event data is fetched from Domain Controllers.



Note: Domain Controllers can also be added from the link "Add Domain Controllers" at the bottom of each Domain Details.

Alerts

In-order to manage alerts that are displayed in ADAudit Plus. An option to manually "delete" or "clear" configured alerts is facilitated with ADAudit Plus from the "Alert" Tab.

The deletion of alerts can also be automated. This is done by scheduling a delete alert from the "Admin" Tab of ADAudit Plus.

To schedule delete alerts

1. Click on the "Admin" Tab -->> Alerts
2. Provide a check against "**Schedule Delete Alerts**"
3. Enter the number of days in the box provided against Delete Alerts older than.
4. Click on Save.

This will schedule a delete alert action and alerts older than the entered number of days will be deleted.

Schedule Reports

Once a report is created, schedules can be set up in ADAudit Plus to run the selected reports automatically at specified time intervals. ADAudit Plus can also be configured to automatically email the report once it runs at desired time intervals.

The reports scheduled to run are generated and stored at a user defined storage path. These reports can be e-mailed as a compressed zip file, a link or as an attachment in any of the listed formats - pdf, xls, csv or html.

To Schedule a New Report

- Click on the "Admin" Tab -->> "Schedule Reports" under Administration -->> "Schedule New Reports"
- Enter the "Schedule Name" and the "Description" for the schedule in the respective Text boxes.
- Select the "Domain Name" from the Drop Down.

Attribute	Description
Schedule Name	Enter a unique name to identify this schedule
Description	Enter a description corresponding to the schedule name.
Domain Name	Select the Domain Name from the drop down. The Drop Down lists all configured Domain names.

Scheduler Creation

Once the schedule name, its description and the domain where the schedule is to be run is defined, the actual schedule creation needs to be done. The Scheduler Creation section of ADAudit Plus discusses about.





Select Reports	Select one or more "Available Reports" to be scheduled under the given "Schedule Name". Both default and User defined Reports can be added to the "Selected Reports" by clicking on the "Add>>" link.
Schedule Report Frequency	The "Selected Reports" can be scheduled on a 'Hourly', 'Daily', 'Weekly' or 'Monthly' basis. The report is scheduled to run once for the frequency selected.
Schedule Report Format	The Scheduled Reports can be stored in 'pdf', 'xls', 'html', or 'csv' formats. They are stored at the "File Storage Path" entered by click on the "File Storage Path" link.
Email Notification	The scheduled report can be e-mailed to any email-id entered in the "specify email address" box on providing a check against "Email this scheduled report".

Select Reports

ADAudit Plus allows you to select one or more reports to be run at scheduled times. The selection of all reports that are to be scheduled is done here. Both user defined and default reports can be selected from the list of available reports by click on the "Add" link against the respective reports.

On clicking the "Add" link, the reports under the "Available Reports" column are selected and moved to the "Selected Reports" column.

On clicking the "Remove" link, the reports selected and listed under the "Selected Reports" column are unselected and moved to the "Available Reports" column.

	<ul style="list-style-type: none"> • Move your cursor on the "Available Reports" table and click on the icon  to select user(s), on the icon  to select computer(s) or on the icon  to select group(s). The icons are displayed only against the reports that require granular object selection. • The objects selected can also be removed by using the "more" link of the "Selected Reports" table.
---	--

Schedule Report Frequency

Different schedules will require different frequencies to be selected and this is facilitated here. ADAudit Plus allows to select the below frequencies.

The schedule can be selected for daily, weekly or hourly by selecting the respective radio buttons.

Frequency	Description
Hourly	If you want to schedule this report to run every hour, enter the time after which this report has to run every one hour.
Daily	If you want to schedule this report to run every day, enter the time at which this report has to run every day. With data being fetched 24 hours from time of schedule (or) The previous day (0:00 hours to 23:59 hours)
Weekly	If you want to schedule this report to run every week, enter the date and time at which this report has to run every week. With data being fetched 7 days from day of schedule (or) The previous week (Monday to Sunday).
Monthly	If you want to schedule this report to run every month, enter the day and time at which this report has to run every month. With data being fetched 30 days from day of schedule (or) The previous month (Day 1 to Day 30).

Provided below are the steps to schedule an hourly report

"Selected Reports" or the "Schedule" will be scheduled to run once every hour.

To set the frequency of the schedule to "Hourly".

- Select the "Hourly" Radio option under "Schedule Report Frequency"
- Enter the Starting time for the Schedule. This schedule will be run on a Hourly basis from the start time selected.

<ul style="list-style-type: none"> • Previous Hour - When a user selects the "Last Hour" option from the drop down. The data will be fetched once every time the clock ticks a valid hour. Eg. (9:00 O' Clock, 10:00 O' clock etc.,) • Last 60 minutes - This depends on the start time selected. The data will be fetched exactly 1 hour (60 minutes) from the time selected as start time.
--

Schedule Report Format

The Scheduled Reports can be stored in 'pdf', 'xls', 'html', or 'csv' formats by selecting the format of choice from the drop down.

They are stored at the "File Storage Path" entered by click on the "File Storage Path" link.

1. The default "File Storage Path" is ' %Product Home Folder%\webapps\adap\schedule-reports\ '. The user can change the storage path for the scheduled reports to any desired location.
2. The "File Server Path" is ' \\file-server\share-folder\ '
3. Outside the product it is 'D:\ADAudit Plus\schedule-reports\ '



If you modify the default "File storage path", scheduled reports cannot be viewed through the web console.

Email Notification

The scheduled report can be sent to any email-id entered in the text box "specify email address" on providing a check against "Email this scheduled report".

Email Notification requires

1. Configuring the "Message Settings"
2. Emailing the Scheduled Report

Message Settings

The "Message Settings" needs to be configured to define the text message and the format (link or attachment) in which the scheduled report will be delivered to a users email id.

To configure the "Message Settings"

- Click on the "Message Settings" link under Email Notification
- Select the options of your choice from the pop-up menu that is displayed.
- Enter the Mail content Entering the " Subject" and "Message" in their respective boxes provided.
- Click on OK.

Options selected to email or publish a scheduled report:

Email Reports as an attachment	Reports are emailed as an attachment. The format of choice is selected under "Schedule Report Format" and could be any of the selected formats pdf, csv, html or xls.
Email Reports as a Zip File	The selected reports are compressed to a zip format and emailed.
Publish the report and email the link alone	Selecting this option the reports are published and the published link alone is emailed to users.

Emailing a Scheduled Report:

To notify a scheduled report by email:

- Provide a check against "Email this scheduled report" under Email Notification section.
- Specify email address in the Text box that is displayed.
- Click on save.

This will email the scheduled report in the desired format (selected under "message settings") to all entered email addresses.

Archive Settings

The Archive Settings of ADAudit Plus allows to archive audit data to a file. It creates a new file for the time provided and compresses the files to a zip format at the intervals mentioned.

To Enable Archiving

1. Click on "Admin" Tab -->> "Archive Settings"
2. Provide a check against "Enable Archiving"
3. Enter the "New File creation interval" (Hours) in the box provided.
4. Enter the "New Zip creation interval" (Hours) in the box provided.
5. Enter the "Archive Directory" in the box provided.
6. Click on "Save".

The archive data are stored at a user defined location. By default the archive files and zip are stored at "**C:\Program Files\AdventNet\ADAudit Plus\archive**"

Event Cleanup

Processed event log data older than what is required for immediate audit reporting can be cleared from the ADAudit Plus database and archived. Event log data are categorized or stratified under the below mentioned categories.

- User Modification,
- Account Creation
- Computer Modification
- Account Logon
- Group Modification
- Domain Policy Changes

ADAudit Plus allows category wise filtering and archiving of processed event log data collected in its database. It also allows one to specify different time periods (days) for clearing processed event log data from each of those categories.

To enable event cleanup

- Click on the "Admin" Tab --> "Event CleanUp" 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.



Only event log data that are processed by ADAudit Plus are cleared from its immediate database. The archived data are stored at the location provided under [Archive Settings](#) of ADAudit Plus.

Technician Settings

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.

Any number of help desk technicians can be added from the admin tab of ADAudit Plus.

To add a help desk technician

1. Login as an admin user
2. Click on the Technicians link under the Admin tab of ADAudit Plus
3. Click on "Add New Technician" Link
4. Select the Domain
5. Choose the User and
6. Select the Role for the selected User.
7. Click on Save

A role has now been delegated to the selected user.

When the user who is delegated an "admin" role logs into ADAudit Plus console.

He has complete privileges of the administrator and will be able to make configuration changes, view reports, schedule reports, view alerts, schedule alerts, perform other admin functions that ADAudit Plus provides. The user who is delegated an admin privilege can modify his and other user roles as well.

When the user who is delegated an "operator" role logs in into ADAudit Plus console

He has the privilege to view reports, view alerts and view charts from ADAudit Plus console.

Troubleshooting Tips

Domain Settings

1. When I start ADAudit Plus, none of my domains are discovered. It says "No Domain Configuration available". Why?
2. When I add my domains manually, the Domain Controllers are not resolved. Why?
3. When I add the Domain Controller, I get an error as "The Servers are not operational". What does it mean?
4. When I add the Domain Controller, I get an error as "Unable to get domain DNS / FLAT name". What does it mean?
5. The status column in the domain settings says that the user do not have Admin Privilege?

Reports

1. My reports show - "No Data Available". Why?

1. When I start ADAudit Plus, none of my domains are discovered. It says "No Domain Configuration available". Why?

ADAudit Plus, upon starting, discovers the domains from the DNS Server associated with the machine running the product. If no domain details are available in the DNS Server, it shows this message.

2. When I add my domains manually, the Domain Controllers are not resolved. Why?

When the DNS associated with the machine running ADAudit Plus do not contain the necessary information. You need to add the Domain Controllers manually.

3. When I add the Domain Controller, I get an error as "The Servers are not operational". What does it mean?

This error could be due to any of the following reasons:

1. DCs are down.
2. Servers not available.
3. Firewall has been enabled, and port 389 is closed.
4. Busy - try after some time?

4. When I add the Domain Controller, I get an error as "Unable to get domain DNS / FLAT name". What does it mean?

This error could be due to any of the following reasons:

1. When the specified user name or the password is invalid.
2. Anonymous login (when no user name and password is provided)
3. When IP Address of the Domain Controller is specified instead of its name.

5. The status column in the domain settings says that the user do not have Admin Privilege?

This is a warning message to indicate that the specified user do not have administrator privileges i.e, the user is not a member of Domain Admins Group. Hence permissions applicable to Administrator may not be available to this user.

Reports

1. My reports showing - "No Data Available". Why?

Possible reasons:

1. Event collection is yet to happen or needs to be initiated.
2. "Domain Auditing Policy" might not have been enabled.
3. Proper / Privileged user credentials were not provided in ADAudit Plus.
4. Your Domain Controller Security Event log settings and ADAudit Plus event Fetch Interval.
5. Currently ADAudit Plus does not support non-English operating systems.

Troubleshooting steps:

1. Event collection is yet to happen or needs to be initiated.

ADAudit Plus has a default "Event Fetch Interval" for it to collect event log data from configured Domain Controllers . This is used for the collection of event logs periodically.


You can manually initiate this event log collection by clicking on the "Domain Settings" link, at the top right corner of the web console and click on "Run Now" link found adjacent to each Domain Controller. This will initiate event fetch from the configured Domain controller, Now check for data in reports.

2. Domain Auditing Policy might not have been enabled.

Ensure that your **Domain Auditing Policy** is enabled. Steps to enable Auditing Policy manually - [Click here](#).

3. Proper / Privileged user credentials were not provided in ADAudit Plus settings.

Proper privileged user credentials are needed for ADAudit Plus to collect event log data from configured Domain Controllers. Steps to provide right user credentials.

1. Go to "Domain Settings"
2. Click on  "Modify Domain Credentials" icon .
3. Enter a privileged credential, a minimum of a user from "**Domain Admin**" group.

4. Your Domain Controller Security Event log settings and ADAudit Plus event Fetch Interval.

If the "**Security Event Log size**" is set to a smaller value, "**Event Fetch interval**" of ADAudit Plus remains at the default 2 hrs and "**Overwrite events as needed**" was enabled on your "**Domain Controller Event log settings**" there is a higher probability of event log data getting lost.

To overcome this :

Ensure that the size of the Domain controller "**Security**" event log is large enough. (You may set the value of Security event log to **at-least** a default value of **130 MB**.)

5. Currently ADAudit Plus does not support non-English operating systems.

Currently ADAudit Plus does not **support non-English operating systems**. If your configured Domain Controllers are of non-English operating systems ADAudit Plus cannot operate. But, it still can be installed on a non-English operating system and collect event logs from Domain Controllers running English operating systems.

Known Issues and Limitations

1. ADAudit Plus presently does not support reporting on Log-Off details for Users.
2. There may be some lacking in handling special characters.