ManageEngine ADAudit Plus

A detailed walkthrough
Agenda

• ManageEngine ADAudit Plus is a web based Active Directory change Audit and Reporting software.

• It helps audit and track all changes in the Active Directory.

• Active Directory changes on Users, Computers, Groups, GPOs, Ous, Domain Policies and logon activities are audited and reported from a central web console.
ADAudit Plus functioning
Tabs in ADAudit Plus

- Home
- Reports
- Alerts
- Configuration
- Admin
- Support
Home Tab of ADAudit Plus
The Home Tab of ADAudit Plus provides a high-level picture with snapshots highlighting important Active Directory audit events like:

1. A graph on the Logon Failure counts in the past 7 / 30 days.
2. A pie-chart highlighting the error-codes when users logon has failed.
3. The count of account locked-out users in the past week / month on a day to day basis.
4. A single bar chart highlighting password changed / set users on a day-to-day basis for the last 7 / 30 days. (Selectable)
Dashboard / Home Tab of ADAudit Plus

• Other Dashboard charts / graphs

1. Peak Logon hour of a day with the average logon count for every hour.
2. Account (user, computer and group) management actions like created, deleted and modified all available on a single graphical interface.

The charts can be clicked to get a list view of desired change data.
Further the graphs are selectable.
The Dashboard provides the above highlighted info for all configured Domain controllers.
Dashboard view of ADAudit Plus

The Home page provides a snapshot of important change actions for all Domains configured on a single screen.

Click on any of the chart to view a list of its underlying details.

Use the refresh Icon to get updated information.

A 30 day or 7 day information can be interchably selected and viewed.
ADAudit Plus Reports Tab
Also explained configuration of Reports
ADAudit Plus Reports

- Default reports - 33 Default reports on Active Directory change actions grouped under 8 different categories are listed.
- Profile based reports – Default reports are associated with an domain object to form Profile based reports.
- Profile based reports are both pre-configured and custom configurable using the configuration tab.
- ADAudit Plus provides over 36 pre-configured profile based reports (under the 8 categories) and innumerable custom-configurable profile based reports or report profiles are listed.
- My Reports – Each report configured by the admin is listed under “My Reports”. Innumerable number of reports can be configured.
ADAudit Plus provides 33 default reports categorized under the below listed 8 categories.

- User Logon Reports
- Local Logon Logoff
- User Management Reports
- Group Management
- Computer Management
- Domain Policy changes
- OU Management
- GPO Management
User Logon Report Category

• The reports under this category provide general logon information of users.

• Information like logon failures, logon attempts on various resources like workstations, member servers are reported and also graphically highlighted.

• Click on the charts above the list to view filtered information.

• Use the add/ remove columns link to add/remove the column of interest.

• The reports can be exported to xls, csv, csvde, pdf and html formats.

• It can be scheduled and configured to email notified to one or more domain users.
User Logon Report Category

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

Pre-configured default user logon reports provide the below information on logon events.
Logon Failure Report

- The logon failure report is a default report under the User Logon Reports category.

- ADAudit Plus collects information on all the logon failures in the selected domain and lists them in a single report.

- A pie-chart highlighted above the list provides a snapshot on all failure reasons.

- The following report highlights the logon failure of all users in the domain “child.admp.com” in the last 24 hours.

- Note: you can also choose custom periods to see varied logon failure reasons for all users.
Logon Failure Report

The change reports in ADAudit Plus are categorized and listed.

The reports can be exported to various formats, you include your own annotations and also print them.
Quick search can be used for identifying change information on specific objects.
To view the available list of scheduled reports and create new schedules click here.
Filter and view information only for what you require.

Graphs highlight – important and desired change information for easy understanding.
### User Logon Activity

Selection of Period for last 24 hours, today, yesterday or any custom period is possible.

#### User Logon Activity

(From Sep 15, 2009 10:25 PM to Sep 16, 2009 10:25 PM)

**Select Domain**: admp.com

**Select User(s)**: test, GuestPL

**Period**: Last 24 Hours

---

#### User Logon Activity

**COUNT**

<table>
<thead>
<tr>
<th>HOUR</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**User Logon Activity**

<table>
<thead>
<tr>
<th>User Name</th>
<th>Client IP Address</th>
<th>Client Host Name</th>
<th>Domain Controller</th>
<th>Logon Time</th>
<th>Event Type</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>127.0.0.1</td>
<td>admp-dcl</td>
<td>admp-dcl</td>
<td>Sep 16, 2009 06:30:57 PM</td>
<td>Success</td>
<td>-</td>
</tr>
<tr>
<td>Administrator</td>
<td>127.0.0.1</td>
<td>admp-dcl</td>
<td>admp-dcl</td>
<td>Sep 16, 2009 01:50:07 PM</td>
<td>Success</td>
<td>-</td>
</tr>
<tr>
<td>Administrator</td>
<td>192.168.116.24</td>
<td>admp-sg07.zohocorp.com</td>
<td>admp-dcl</td>
<td>Sep 16, 2009 12:09:46 PM</td>
<td>Success</td>
<td>-</td>
</tr>
</tbody>
</table>
Recent User Logon Activity - Status

Select Domain: admnp.com

Period: Custom Period

Start Time: 2009-09-11 12:00 AM
End Time: 2009-09-11 12:00 AM

Recent User Logon Activity

<table>
<thead>
<tr>
<th>User Name</th>
<th>Client IP Address</th>
<th>Client Host Name</th>
<th>Domain Controller</th>
<th>Logon Time</th>
<th>Event Type</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>192.168.116.25</td>
<td>admin-ex07.zohocorp.com</td>
<td>admnp-dc1</td>
<td>Sep 15, 2009 08:15:02 PM</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td>192.168.116.24</td>
<td>admin-ex07.zohocorp.com</td>
<td>admnp-dc1</td>
<td>Sep 15, 2009 07:36:56 PM</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td>127.0.0.1</td>
<td>admnp-dc1</td>
<td>admnp-dc1</td>
<td>Sep 15, 2009 04:14:43 PM</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td>127.0.0.1</td>
<td>admnp-dc1</td>
<td>admnp-dc1</td>
<td>Sep 15, 2009 04:41:48 PM</td>
<td>Failure</td>
<td>Bad password</td>
</tr>
<tr>
<td>Administrator</td>
<td>127.0.0.1</td>
<td>admnp-dc1</td>
<td>admnp-dc1</td>
<td>Sep 15, 2009 02:40:33 PM</td>
<td>Success</td>
<td></td>
</tr>
</tbody>
</table>
Last Logon on Workstations – User’s last login info

Connected Domain: adm0.com

Last Logon on Workstations

Select Domain: adm0.com

Period: Custom Period

Start Time: 2008-03-01 12:00 AM
End Time: 2009-09-30 12:00 AM

<table>
<thead>
<tr>
<th>User Name</th>
<th>Client IP Address</th>
<th>Client Host Name</th>
<th>Domain Controller</th>
<th>Logon Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>192.160.116.23</td>
<td>edcpe-ex07.zohocorp.com</td>
<td>edm0-dc1</td>
<td>Sep 15, 2009 00:54:00 AM</td>
</tr>
<tr>
<td>Administrator</td>
<td>192.160.116.24</td>
<td>edm0-ex07.zohocorp.com</td>
<td>edm0-dc1</td>
<td>Sep 15, 2009 07:36:56 AM</td>
</tr>
<tr>
<td>Administrator</td>
<td>192.160.116.31</td>
<td></td>
<td>edm0-dc1</td>
<td>Sep 15, 2009 04:41:49 AM</td>
</tr>
<tr>
<td>dcondemand</td>
<td>192.160.117.145</td>
<td>dccloud-xp1.zohocorp.com</td>
<td>edm0-dc1</td>
<td>Sep 10, 2009 12:33:52 PM</td>
</tr>
<tr>
<td>dcondemand</td>
<td>192.160.117.123</td>
<td>dccloud-xp2.zohocorp.com</td>
<td>edm0-dc1</td>
<td>Sep 10, 2009 02:05:55 AM</td>
</tr>
<tr>
<td>Administrator</td>
<td>192.160.116.23</td>
<td>edm0-dc1.zohocorp.com</td>
<td>edm0-dc1</td>
<td>Sep 04, 2009 04:06:16 AM</td>
</tr>
<tr>
<td>Administrator</td>
<td>192.160.117.204</td>
<td>edm0-vista64.zohocorp.com</td>
<td>edm0-dc1</td>
<td>Sep 03, 2009 02:26:59 PM</td>
</tr>
<tr>
<td>Administrator</td>
<td>192.168.117.114</td>
<td>192.168.117.114</td>
<td>edm0-dc1</td>
<td>Aug 31, 2009 04:08:35 PM</td>
</tr>
<tr>
<td>Administrator</td>
<td>192.160.117.152</td>
<td>edm0-vista2.zohocorp.com</td>
<td>edm0-dc1</td>
<td>Aug 03, 2009 12:32:19 PM</td>
</tr>
</tbody>
</table>
# User’s Last Logon – computer info.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Logon Time</th>
<th>Client IP Address</th>
<th>Client Host Name</th>
<th>Domain Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Sep 15, 2009 08:54:02 PM</td>
<td>122.160.116.25</td>
<td>admphost07.zohocorp.in.com</td>
<td>admph-dc1</td>
</tr>
<tr>
<td>IUSR_ADMPP-DC1</td>
<td>Sep 15, 2009 02:00:40 AM</td>
<td>127.0.0.1</td>
<td></td>
<td>admph-dc1</td>
</tr>
<tr>
<td>test44</td>
<td>Sep 12, 2009 12:56:20 AM</td>
<td>127.0.0.1</td>
<td></td>
<td>admph-dc1</td>
</tr>
<tr>
<td>test133</td>
<td>Sep 11, 2009 06:49:23 AM</td>
<td>127.0.0.1</td>
<td></td>
<td>admph-dc1</td>
</tr>
<tr>
<td>dcodeamdemand</td>
<td>Sep 10, 2009 12:30:52 AM</td>
<td>122.160.117.145</td>
<td>dcodeamdemand.zohocorp.in.com</td>
<td>admph-dc1</td>
</tr>
<tr>
<td>testuser2</td>
<td>Sep 09, 2009 04:26:20 AM</td>
<td>127.0.0.1</td>
<td></td>
<td>admph-dc1</td>
</tr>
<tr>
<td>test277</td>
<td>Sep 08, 2009 01:57:17 AM</td>
<td>127.0.0.1</td>
<td></td>
<td>admph-dc1</td>
</tr>
<tr>
<td>TestMailboxUser1</td>
<td>Sep 03, 2009 08:16:20 AM</td>
<td>127.0.0.1</td>
<td></td>
<td>admph-dc1</td>
</tr>
<tr>
<td>user1</td>
<td>Sep 02, 2009 02:46:26 PM</td>
<td>127.0.0.1</td>
<td></td>
<td>admph-dc1</td>
</tr>
<tr>
<td>test2</td>
<td>Sep 02, 2009 02:10:28 PM</td>
<td>127.0.0.1</td>
<td></td>
<td>admph-dc1</td>
</tr>
</tbody>
</table>
Local Logon-Logoff Reports

- Logon Duration on DCs
- Logon Failures on DCs
- Logon History of DCs
- Terminal Services Activity on DCs

Pre-configured default reports on local logon-logoff actions on domain controllers (DCs) are listed above.
Logon Failure on DCs

Logon Failures on DCs

Select Domain: adm.com
Select Domain Controller(s): ADMP-DC1, ADMP-DC2
Period: Custom Period
Start Time: 10/8/2009 12:00 AM
End Time: 10/8/2009 12:00 AM

Filter based on inputs: All

Top User Logon Failures on DCs

<table>
<thead>
<tr>
<th>Username</th>
<th>Client IP Address</th>
<th>Client Host Name</th>
<th>Domain Controller</th>
<th>Logon Time</th>
<th>Event Type</th>
<th>Remarks</th>
<th>Logon Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator</td>
<td>192.168.4.220</td>
<td>met6.adappscan.com</td>
<td>ADMP-DC1</td>
<td>Oct 10, 2009 03:20:16 PM</td>
<td>Failure</td>
<td>Unknown user name or bad password</td>
<td>Remote Interactive (Terminal Services, Remote Desktop or Remote Assistance)</td>
</tr>
<tr>
<td>administrator</td>
<td>192.168.119.161</td>
<td>dcwww.w1.spl.zohorscorpin.com</td>
<td>ADMP-DC1</td>
<td>Oct 10, 2009 01:59:13 PM</td>
<td>Failure</td>
<td>Unknown user name or bad password</td>
<td>Unlock (i.e., unauthorized workstation with password protected screen saver)</td>
</tr>
</tbody>
</table>
Logon History of DCs

Logon History of DCs
(From Jul 01, 2009 12:00 AM to Oct 12, 2009 12:00 AM)

<table>
<thead>
<tr>
<th>User Name</th>
<th>Client IP Address</th>
<th>Client Host Name</th>
<th>Domain Controller</th>
<th>Login Time</th>
<th>Event Type</th>
<th>Remarks</th>
<th>Logon Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator</td>
<td>192.168.4.220</td>
<td>RAGHURAMAN B</td>
<td>admp-dc1</td>
<td>Oct 10, 2009 05:20:12 PM</td>
<td>Success</td>
<td>Session disconnected from workstation</td>
<td>Remote Interactive (Terminal Services, Remote Desktop or Remote Assistance)</td>
</tr>
<tr>
<td>administrator</td>
<td>192.168.4.220</td>
<td><a href="mailto:net@zohocorp.in.com">net@zohocorp.in.com</a></td>
<td>admp-dc1</td>
<td>Oct 10, 2009 05:20:13 PM</td>
<td>Success</td>
<td>Successful Logon</td>
<td>Remote Interactive (Terminal Services, Remote Desktop or Remote Assistance)</td>
</tr>
<tr>
<td>administrator</td>
<td>192.168.4.220</td>
<td><a href="mailto:net@zohocorp.in.com">net@zohocorp.in.com</a></td>
<td>admp-dc1</td>
<td>Oct 10, 2009 05:20:16 PM</td>
<td>Failure</td>
<td>Unknown username or bad password</td>
<td>Remote Interactive (Terminal Services, Remote Desktop or Remote Assistance)</td>
</tr>
<tr>
<td>administrator</td>
<td>-</td>
<td>-</td>
<td>admp-dc1</td>
<td>Oct 10, 2009 05:19:22 PM</td>
<td>Success</td>
<td>User initiated logout</td>
<td>-</td>
</tr>
<tr>
<td>administrator</td>
<td>-</td>
<td>-</td>
<td>admp-dc1</td>
<td>Oct 10, 2009 05:20:12 PM</td>
<td>Success</td>
<td>Unlock the unattended</td>
<td>-</td>
</tr>
</tbody>
</table>
Terminal Services Activity on DCs

(From Aug 01, 2009 12:00 AM to Oct 12, 2009 12:00 AM)

Select Domain: admp.com
Select Domain Controller(s): ADMP-DCL, ADMP...
Period: Custom Period
Start Time: 2009-08-01 12:00 AM
End Time: 2009-10-1 12:00 AM

Filter based on inputs: All

Displaying report for input entries: ADMP-DCL, ADMP...

Terminal Services Activity on DCs

Quick Search
Showing: 1-25 of 120
Show 25

<table>
<thead>
<tr>
<th>User Name</th>
<th>Client IP Address</th>
<th>Client Host Name</th>
<th>Domain Controller</th>
<th>Login Time</th>
<th>Event Type</th>
<th>Remarks</th>
<th>Logon Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator</td>
<td>192.168.4.220</td>
<td>RAGHURAMAINB</td>
<td>admp-dcl</td>
<td>Oct 10, 2009 09:58:12 PM</td>
<td>Success</td>
<td>Session disconnected from workstation</td>
<td>Remote Interactive (Terminal Services, Remote Desktop or Remote Assistance)</td>
</tr>
<tr>
<td>administrator</td>
<td>192.168.4.220</td>
<td>net6.cohoncinm.com</td>
<td>ADMP-DCL</td>
<td>Oct 10, 2009 09:20:16 PM</td>
<td>Failure</td>
<td>Unknown user name or bad password</td>
<td>Remote Interactive (Terminal Services, Remote Desktop or Remote Assistance)</td>
</tr>
</tbody>
</table>
User Management Reports

- Recently Created Users
- Recently Deleted Users
- Recently Enabled Users
- Recently Disabled Users
- Recently Locked Out Users
- Recently Unlocked Users
- Recently Modified Users

Preconfigured default reports under the user management category are listed above.

- Recently Password Changed Users
- Recently Password Set Users
- Password Never Expires Set Users
- Last Modification on Users
- Administrative User Actions
- User Object History

Preconfigured default reports under the user management category are listed above.
User Management Reports

- All reports follow similar pattern and it is easy for one to understand all reports by just viewing one.
- Recently Created Users, Recently Deleted Users, Recently Enabled Users, Recently Disabled Users, Recently Locked Out Users, Recently Unlocked Users, Recently Modified Users, Recently Password Changed Users, Recently Password Set Users.
- The last modification on user report lists the last change that was done on every user in the domain.
- Administrative User Actions – covers all administrative actions done by selected user(administrator or helpdesk) in the domain on users, computers and groups.
- User object history lists all the history of changes that happened on selected user(s).
Recently created users report

<table>
<thead>
<tr>
<th>User Name</th>
<th>SAH Account Name</th>
<th>Caller User Name</th>
<th>Creation Time</th>
<th>Domain Controller</th>
<th>User Principal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>test90</td>
<td>test90</td>
<td>administrator</td>
<td>Aug 24, 2020 03:07:29 PM</td>
<td>emp-dci.dhis.change.com</td>
<td><a href="mailto:test90@dhis.change.com">test90@dhis.change.com</a></td>
</tr>
<tr>
<td>testuser44.text</td>
<td>testuser44.text</td>
<td>administrator</td>
<td>Mar 10, 2009 16:47:16 AM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>testuser22.test</td>
<td>testuser22.test</td>
<td>administrator</td>
<td>Mar 10, 2009 16:35:16 AM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>testuser44.text</td>
<td>testuser44.text</td>
<td>administrator</td>
<td>Mar 10, 2009 16:35:49 AM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>toothfuser14</td>
<td>toothfuser14</td>
<td>administrator</td>
<td>Mar 10, 2009 16:21:37 AM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>toothfuser23</td>
<td>toothfuser23</td>
<td>Administrator</td>
<td>Mar 10, 2009 16:07:03 AM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>servicedesk</td>
<td>servicedesk</td>
<td>administrator</td>
<td>Mar 07, 2009 02:50:26 PM</td>
<td>emp-dci.dhis.change.com</td>
<td><a href="mailto:servicedesk@dhis.change.com">servicedesk@dhis.change.com</a></td>
</tr>
<tr>
<td>BOR95621</td>
<td>BOR95621</td>
<td>Administrator</td>
<td>Mar 06, 2009 02:52:16 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>BOR90621</td>
<td>BOR90621</td>
<td>Administrator</td>
<td>Mar 06, 2009 02:50:16 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>BOR95621</td>
<td>BOR95621</td>
<td>Administrator</td>
<td>Mar 06, 2009 02:49:40 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>BOR20211</td>
<td>BOR20211</td>
<td>Administrator</td>
<td>Mar 06, 2009 02:49:48 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>firstmid123</td>
<td>firstmid123</td>
<td>Administrator</td>
<td>Mar 04, 2009 04:16:04 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>firstmid23</td>
<td>firstmid23</td>
<td>Administrator</td>
<td>Mar 04, 2009 04:16:04 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>last_mid_first</td>
<td>last_mid_first</td>
<td>Administrator</td>
<td>Mar 04, 2009 04:12:57 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>last_mid_first</td>
<td>last_mid_first</td>
<td>Administrator</td>
<td>Mar 04, 2009 04:12:57 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>techmonitor2</td>
<td>techmonitor2</td>
<td>Administrator</td>
<td>Mar 03, 2009 03:02:01 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>techmonitor2</td>
<td>techmonitor2</td>
<td>Administrator</td>
<td>Mar 03, 2009 03:02:01 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
<tr>
<td>techmonitor2</td>
<td>techmonitor2</td>
<td>Administrator</td>
<td>Mar 03, 2009 03:02:01 PM</td>
<td>emp-dci.dhis.change.com</td>
<td></td>
</tr>
</tbody>
</table>
Last Modification on User(s)

(From Sep 13, 2009 02:33 PM to Oct 13, 2009 02:33 PM)

Select Domain: adm.com
Period: Last 30 Days

<table>
<thead>
<tr>
<th>User Name</th>
<th>Caller User Name</th>
<th>Modified Time</th>
<th>Domain Controller</th>
<th>Modified Attributes</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>payun</td>
<td>Administrator</td>
<td>Oct 10, 2009 10:59:13 AM</td>
<td>adm-oc1</td>
<td>User Workstations</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>Anand</td>
<td>Administrator</td>
<td>Oct 10, 2009 07:38:52 AM</td>
<td>adm-oc1</td>
<td>User Principal Name</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>az</td>
<td>administrator</td>
<td>Oct 09, 2009 01:29:08 PM</td>
<td>adm-oc1</td>
<td>User Parameters</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>Allen</td>
<td>Administrator</td>
<td>Oct 10, 2009 09:34:24 AM</td>
<td>adm-oc1</td>
<td>User Account Control</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>Anand</td>
<td>Administrator</td>
<td>Oct 09, 2009 06:03:21 AM</td>
<td>adm-oc1</td>
<td>User Account Control</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>Anand</td>
<td>Administrator</td>
<td>Oct 09, 2009 06:43:56 AM</td>
<td>adm-oc1</td>
<td>User Account Control</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>Anand</td>
<td>Administrator</td>
<td>Oct 09, 2009 08:43:12 AM</td>
<td>adm-oc1</td>
<td>User Account Control</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>audituser</td>
<td>Administrator</td>
<td>Oct 09, 2009 06:32:04 AM</td>
<td>adm-oc1</td>
<td>User Account Control</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>bala</td>
<td>Administrator</td>
<td>Oct 05, 2009 02:46:59 PM</td>
<td>adm-oc1</td>
<td>User Account Control</td>
<td>User Account Changed</td>
</tr>
<tr>
<td>dcondemand</td>
<td>administrator</td>
<td>Oct 12, 2009 07:59:08 AM</td>
<td>adm-oc1</td>
<td>User Account Control</td>
<td>User Account Changed</td>
</tr>
</tbody>
</table>
Administrative User Action – on user objects

Administrative user action computer and group objects are similar.
### User Object History

**From Sep 13, 2009 82:41 PM to Oct 13, 2009 82:41 PM**

**Filter based on inputs**

- Select Domain: admnp.com
- Select User(s): test, CurrentPl...
- Period: Last 30 Days

#### User Object History

![Pie Chart]

- User Account Changed
- User Account Created
- User Account Disabled
- User Account Enabled
- User Account Password Set
- User Account Unlocked

<table>
<thead>
<tr>
<th>Modified Time</th>
<th>Domain Controller</th>
<th>Description</th>
<th>Remarks</th>
<th>Event Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 12, 2009 11:45:38 PM</td>
<td>admnp-dc1</td>
<td>User account 'Administrators' was changed by 'ADMIPARM DCP'. Changed Attributes: 'Password Last Set'.</td>
<td>User Account Changed</td>
<td>642</td>
</tr>
<tr>
<td>Oct 12, 2009 11:56:17 AM</td>
<td>admnp-dc1</td>
<td>User account 'test' was changed by 'ADMIPARM Administrator'. Changed Attributes: 'Password Last Set'.</td>
<td>User Account Changed</td>
<td>642</td>
</tr>
<tr>
<td>Oct 12, 2009 09:46:42 AM</td>
<td>admnp-dc1</td>
<td>User account 'test' was changed by 'ADMIPARM Administrator'. Changed Attributes: 'Password Last Set'.</td>
<td>User Account Changed</td>
<td>642</td>
</tr>
<tr>
<td>Oct 12, 2009 09:15:48 AM</td>
<td>admnp-dc1</td>
<td>User account 'test' was changed by 'ADMIPARM Administrator'. Changed Attributes: 'Password Last Set'.</td>
<td>User Account Changed</td>
<td>642</td>
</tr>
<tr>
<td>Oct 12, 2009 08:53:34 AM</td>
<td>admnp-dc1</td>
<td>User account 'test' was changed by 'ADMIPARM Administrator'. Changed Attributes: 'Account Expires'.</td>
<td>User Account Changed</td>
<td>642</td>
</tr>
<tr>
<td>Oct 12, 2009 07:15:08 AM</td>
<td>admnp-dc1</td>
<td>User account 'davidjohn' was changed by 'ADMIPARM Administrator'. Changed Attributes: 'User Account Control'.</td>
<td>User Account Changed</td>
<td>642</td>
</tr>
<tr>
<td>Oct 12, 2009 06:27:25 AM</td>
<td>admnp-dc1</td>
<td>User account 'user42' was changed by 'ADMIPARM Administrator'. Changed Attributes: 'Password Last Set'.</td>
<td>User Account Changed</td>
<td>642</td>
</tr>
</tbody>
</table>
Group Management Audit Reports

- Recently Created Security Groups
- Recently Created Distribution Groups
- Recently Deleted Security Groups
- Recently Deleted Distribution Groups
- Recently Modified Groups
- Recently Added Members to Security Groups
- Recently Added Members to Distribution Groups
- Recently Removed Members from Security Groups
- Recently Removed Members from Distribution Groups
- Group Object History

Pre-configured default reports on group management actions and history of changes to groups is listed above.
Group Management Audit Reports

- Along with creation, deletion and modification of security and distribution groups. ADAudit Plus provides additional reports on members added/removed to or from these Groups.

- A sample screenshot for the “Group object history” is also provided.
Recently added members to Security Groups

Use this link to add or removed desired columns

Recently Added Members to Security Groups
(From Sep 13, 2009 02:15 PM to Oct 13, 2009 02:15 PM)

Select Domain: admn.com
Period: Last 30 Days

Who added
Member added
Time of addition of a member

Use this link to add or removed desired columns

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Caller User Name</th>
<th>Member Name</th>
<th>Modification Time</th>
<th>Domain Controller</th>
<th>Remarks</th>
<th>Group Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>Administrator</td>
<td>cn=tastthlogin,DC=admn,DC=com</td>
<td>Oct 09 2009 05:14:03 PM</td>
<td>admp-dc1</td>
<td>Security Enabled Local Group</td>
<td>Member Added</td>
</tr>
<tr>
<td>Terminal Server License</td>
<td>Administrator</td>
<td>cn=tastthlogin,DC=admn,DC=com</td>
<td>Oct 09 2009 05:14:03 PM</td>
<td>admp-dc1</td>
<td>Security Enabled Local Group</td>
<td>Member Added</td>
</tr>
<tr>
<td>Remote Desktop Users</td>
<td>Administrator</td>
<td>CN=passwrdajajl, PSAW=UH+D01, OU=AUT, DC=admn,DC=com</td>
<td>Oct 09 2009 05:13:59 PM</td>
<td>admp-dc1</td>
<td>Security Enabled Local Group</td>
<td>Member Added</td>
</tr>
<tr>
<td>Administrators</td>
<td>Administrator</td>
<td>CN=passwrdajajl, PSAW=UH+D01, OU=AUT, DC=admn,DC=com</td>
<td>Oct 10 2009 07:07:15 AM</td>
<td>admp-dc1</td>
<td>Security Enabled Local Group</td>
<td>Member Added</td>
</tr>
<tr>
<td>kittest1</td>
<td>Administrator</td>
<td>CN=kittest1, OU=SKumar, DC=admn,DC=com</td>
<td>Oct 05 2009 02:01:34 PM</td>
<td>admp-dc1</td>
<td>Security Enabled Local Group</td>
<td>Member Added</td>
</tr>
<tr>
<td>kittest2</td>
<td>Administrator</td>
<td>CN=kittest2, OU=SKumar, DC=admn,DC=com</td>
<td>Oct 05 2009 02:02:18 PM</td>
<td>admp-dc1</td>
<td>Security Enabled Local Group</td>
<td>Member Added</td>
</tr>
<tr>
<td>kittest3</td>
<td>Administrator</td>
<td>CN=kittest3, OU=SKumar, DC=admn,DC=com</td>
<td>Oct 05 2009 02:02:18 PM</td>
<td>admp-dc1</td>
<td>Security Enabled Local Group</td>
<td>Member Added</td>
</tr>
<tr>
<td>kittestGroup</td>
<td>administrator</td>
<td>CN=kittest4, OU=SKumar, DC=admn,DC=com</td>
<td>Oct 05 2009 17:48:38 PM</td>
<td>admp-dc1</td>
<td>Security Enabled Local Group</td>
<td>Member Added</td>
</tr>
</tbody>
</table>
Group Object History

This report lists the History of actions on the selected Group(s). The Group created/deleted and modified times. It also lists members added/removed to the selected group object(s).

The scope of the Group is limited to the Domain Selected here.

Use the Add Icon to select more than one Group.
Computer Management Audit Reports

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

Pre-configured default reports on audit actions that occurred on one or all computer objects.
Domain Policy Changes

- Domain policy change report.

This pre-configured report provides detailed change information of a Domain Policy.
Domain Policy change information

Domain Policy Changes
(From Oct 01, 2008 12:00 AM to Oct 15, 2008 12:00 AM)

Select Domain: admp.com

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Domain Controller</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 12, 2008</td>
<td>11:01:21 PM</td>
<td>admp-dc1</td>
<td>Domain Policy Changed; Password Policy modified</td>
</tr>
<tr>
<td>Oct 13, 2008</td>
<td>06:41:31 AM</td>
<td>admp-dc1</td>
<td>Domain Policy Changed; Lockout Policy modified</td>
</tr>
</tbody>
</table>
OU Management Reports

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

Pre-configured default audit reports on OU management actions provided by ADAudit Plus are listed above.
GPO Management Audit Reports

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

Pre-configured default audit reports provided by ADAudit Plus for GPO Management changes are listed above.
Profile Based Reports

- A profile based report is defined by associating one or more Report profiles with one or more Active Directory object(s).
- The advantage of a Profile based report is that it allows viewing specific change information done by or on objects in the Domain.
- For Example: Logon Failure for Admin users (or) Administrative Users Logon Failure
  - Is created by associating
Configuring a Report Profile - 1

List of default Report Profile Categories

Listed are the available report profiles under the Account Logon Report Profile category for domain admp.com.

To configure your own report profile, click here. The report profiles created will be listed under their respective category / domain.

To view a Profile based Report – click on view reports – It will be shown under Reports → Profile based reports.

List of default Report Profile Categories
Configuring a report profile - 2

- **Report profile name**
- **Check only the actions that need to be present in the Profile based report**
- **Actions for the selected category. (Each action be configured under Advanced Configuration)**
- **Deletion of Undesired object for the Profile Based Report**
- **Filter to include only Admin Users for the Domain**
The actions change with the category selected. Listed are categories under which report profiles / profile based reports can be configured.
List of Report Profiles configured by user. Any number of report profiles can be configured. To report on desired changes.

<table>
<thead>
<tr>
<th>Action</th>
<th>Name</th>
<th>Event Date</th>
<th>Event Time</th>
<th>View Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon failure of Domain Admins</td>
<td></td>
<td>Oct 13, 2009 10:45 AM</td>
<td>Oct 16, 2009 02:41 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>user modification for selected 10 users</td>
<td></td>
<td>Oct 13, 2009 10:58 AM</td>
<td>Oct 16, 2009 01:40 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>group/computer/user creation</td>
<td></td>
<td>Oct 13, 2009 10:57 AM</td>
<td>Oct 16, 2009 01:39 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>GPO management for creation</td>
<td></td>
<td>Oct 13, 2009 08:03 AM</td>
<td>Oct 16, 2009 01:39 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>OU management based on all OUs of domain</td>
<td></td>
<td>Oct 13, 2009 08:03 AM</td>
<td>Oct 16, 2009 01:37 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>group modification based on domain group</td>
<td></td>
<td>Oct 13, 2009 08:02 AM</td>
<td>Oct 16, 2009 01:36 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>computer modification on domain</td>
<td></td>
<td>Oct 13, 2009 11:01 AM</td>
<td>Oct 16, 2009 01:35 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>computer modification based on computer</td>
<td></td>
<td>Oct 13, 2009 11:01 AM</td>
<td>Oct 16, 2009 01:35 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>computer modification based on group</td>
<td></td>
<td>Oct 13, 2009 11:01 AM</td>
<td>Oct 16, 2009 01:35 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>computer modification based on OU</td>
<td></td>
<td>Oct 13, 2009 11:02 AM</td>
<td>Oct 16, 2009 01:34 AM</td>
<td>View Reports</td>
</tr>
<tr>
<td>group modification based on ou</td>
<td></td>
<td>Oct 13, 2009 11:03 AM</td>
<td>Oct 16, 2009 01:34 AM</td>
<td>View Reports</td>
</tr>
</tbody>
</table>
### Profile Based Report

**Connected Domains:** admpw2k8.com

**Profile Based Reports:**
- User Logon Reports
- Local Logon-Logoff
- User Management
- Group Management
- Computer Management
- Domain Policy Changes
- OU Management
- Profile Based Reports
- Group, Computer & User creation in admpw2k8.com

#### Period: Last 30 Days

<table>
<thead>
<tr>
<th>New Account Name</th>
<th>New account Domain</th>
<th>Caller username</th>
<th>Caller user domain</th>
<th>Sam Account Name</th>
<th>Creation Time</th>
<th>Object Class</th>
<th>Domain Controller</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMP4$</td>
<td>ADMPW2K8</td>
<td>administrator</td>
<td>ADMPW2K8</td>
<td>COMP4$</td>
<td>07/14/2009</td>
<td>computer</td>
<td>edmpw2k8.admpw2k8.com</td>
<td>A computer account was created</td>
</tr>
<tr>
<td>COMP3$</td>
<td>ADMPW2K8</td>
<td>administrator</td>
<td>ADMPW2K8</td>
<td>COMP3$</td>
<td>07/14/2009</td>
<td>computer</td>
<td>edmpw2k8.admpw2k8.com</td>
<td>A computer account was created</td>
</tr>
<tr>
<td>COMP2$</td>
<td>ADMPW2K8</td>
<td>administrator</td>
<td>ADMPW2K8</td>
<td>COMP2$</td>
<td>07/14/2009</td>
<td>computer</td>
<td>edmpw2k8.admpw2k8.com</td>
<td>A computer account was created</td>
</tr>
<tr>
<td>COMP1$</td>
<td>ADMPW2K8</td>
<td>administrator</td>
<td>ADMPW2K8</td>
<td>COMP1$</td>
<td>07/14/2009</td>
<td>computer</td>
<td>edmpw2k8.admpw2k8.com</td>
<td>A computer account was created</td>
</tr>
<tr>
<td>666</td>
<td>ADMPW2K8</td>
<td>administrator</td>
<td>ADMPW2K8</td>
<td>666</td>
<td>07/14/2009</td>
<td>group</td>
<td>edmpw2k8.admpw2k8.com</td>
<td>A security disabled user was created</td>
</tr>
<tr>
<td>6</td>
<td>ADMPW2K8</td>
<td>administrator</td>
<td>ADMPW2K8</td>
<td>6</td>
<td>07/14/2009</td>
<td>group</td>
<td>edmpw2k8.admpw2k8.com</td>
<td>A security disabled user was created</td>
</tr>
</tbody>
</table>
List of all reports configured by you.
Alerts Tab of ADAudit Plus

Also explained configuration of Alerts
• Receive alerts on desired change events - right in your inbox/ the product.

• Alerts in ADAudit Plus include
  – Default Web Alerts and configurable email notification of the alerts.
  – They are categorized under
    • Alert Profile Based Alerts and
    • Report Profile Based Alerts.
Default Alerts configured in ADAudit Plus

- Logon Failures for Admin Users
- Users Created
- Deleted Users
- Deleted Security Groups
- Modified Admin Groups
- Domain Policy Changes
- OUs Deleted
- GPOs Deleted

Default Web Alerts configured in ADAudit Plus. The alerts are available under both Alert Profile Based Alerts and Report Profile Based Alerts.
What are Alert Profile Based Alerts and Report Profile Based Alerts
An Alert Profile based alert is the alert that you would like to see in totality for a desired change.

- It is configured by combining one or all of the below. Done in the configuration Tab of ADAudit Plus
  - Name
  - Description
  - One or a combination of multiple Report Profiles.
  - An alert message (configurable)
  - If the alert is to be email notified.
Configuring an Alert Profile based Alert

One or all report profiles can be added to be alerted.

Provide a check to email notify the configured alert.

Select the severity from the drop down “Attention”, “Troublesome” or “critical” alert.

Custom configuration of alert message.
Active Alert seen from the product

Consolidated list of all event details configured to be alerted. You will be able to view it just on clicking the Alerts Tab.

Selectable period to view list of alerts received.

Select to view “Active Alerts” or “All Alerts”
Viewing a Alert Profile Based Alert

- Removes the alerted event from Active Alerts. You can still view them under “All alerts”.
- Removes the alert in totality.
- Click on the alert to view complete data for the change event. (See next page.)
What event detail does each alert provide.

This will be the event detail information that you receive when you click on any row in web alert and in your Mailbox with each event occurrence.
This alert is based on “Report Profile”. One or more Report Profile based alerts combine to form an Alert profile based alert. Information is limited to the Domain object.
Advanced Configuration

- Allows you to define actions that are added for a report profile.
- The Actions are based on a combination of one or more Rule-Groups.
- Rule Groups are formed using Rules – using “and” or “or” operators.
- Each Rule is based on specific attributes of Active Directory change.
- ADAudit Plus intelligently understands categories and groups them for defining rules.
Configuring an Action in ADAudit Plus

Any number of Actions can be configured in ADAudit Plus. These are based on Filter rules / rule groups.

The Logon Failure events 2000 AD under Account Logon Actions Category. Is defined using the listed 8 Rule Groups.

Any number of Actions can be configured in ADAudit Plus. These are based on Filter rules / rule groups.
Operators used to define a filter rule.

Any number of Filter Rules can be added.

Attributes for Account Logon actions. This varies depending on the category selected.

Any number of Rule Groups can be added.
Admin Tab of ADAudit Plus
The Admin tab of ADAudit Plus allows you to configure the various settings for working with the product.
This Tab allows you to personalize ADAudit Plus by selecting a theme and changing the default password to desired.
The connections Tab allows you to select the port and to set session expiry. Running ADAudit Plus as a secure connection is possible with this.
Settings required for ADAudit Plus to start and for debugging can be set in this Tab.
Mail Server Settings

Configure Mail Server Settings

- **Mail Server:** SMTP
- **Mail Port:** 25
- **Authentication:**
  - Username: administrator
  - Password: **********
- **Configure EMail Addresses**
  - From Address: noreply@adauditplus.com

Settings required for ADAudit Plus to send emails
The Domain Settings Tab allows to add or remove Domain controllers from which event log data is to be collected.

• The event fetch interval can set and also modified.

• Any number of Domain Controllers can be included - based on license purchase. The trial version fetches event_viewer data from 5 Domain Controllers.
Adding Domain and Domain Controllers

Adding a Domain controller. Multiple DC’s added by separating them using comma.
Schedule Deletion of Alerts

On providing a check again “Schedule Delete Alerts” option. Alerts older than specified number of days are deleted from the Web Alerts displayed.
Archive Settings

Filtered raw event log data are archived under the folder mentioned. The time and folders are configured here.
Scheduled Reports

This report can also be accessed from the Reports Tab on clicking the Schedule Reports Link.

Active Schedule – click to disable
Disabled Schedule – click to enable

Viewing all Scheduled reports

Successfully enabled the scheduled report
Scheduling a Report

One or all available reports can be selected to the list using the add button.

The schedule report frequency allows schedules to be run at specified times for report extraction.

Schedule report Storage path and reported/stored format are provided here.

The scheduled reports will be sent via e-mail if this option is checked. And for the configured settings.
Processed event log data older than the specified number of days are archived and then cleared from the database. Categories that are not checked for Event CleanUp are not cleared.
Multiple Technicians can be allowed to access ADAudit Plus web portal. ADAudit Plus allows to configure any of “Admin” or “Operator” role for the selected technician. An operator will only be able view reports. “Admin” has complete privileges on the product.
Conclusion

• Kindly Visit: http://www.adauditplus.com for more information on product and pricing.

• Take a walk through on the User Interface at http://demo.adauditplus.com

• For any technical queries or assistance contact support@adauditplus.com

• You can contact us also via. Toll Free: 1-888-720-9500