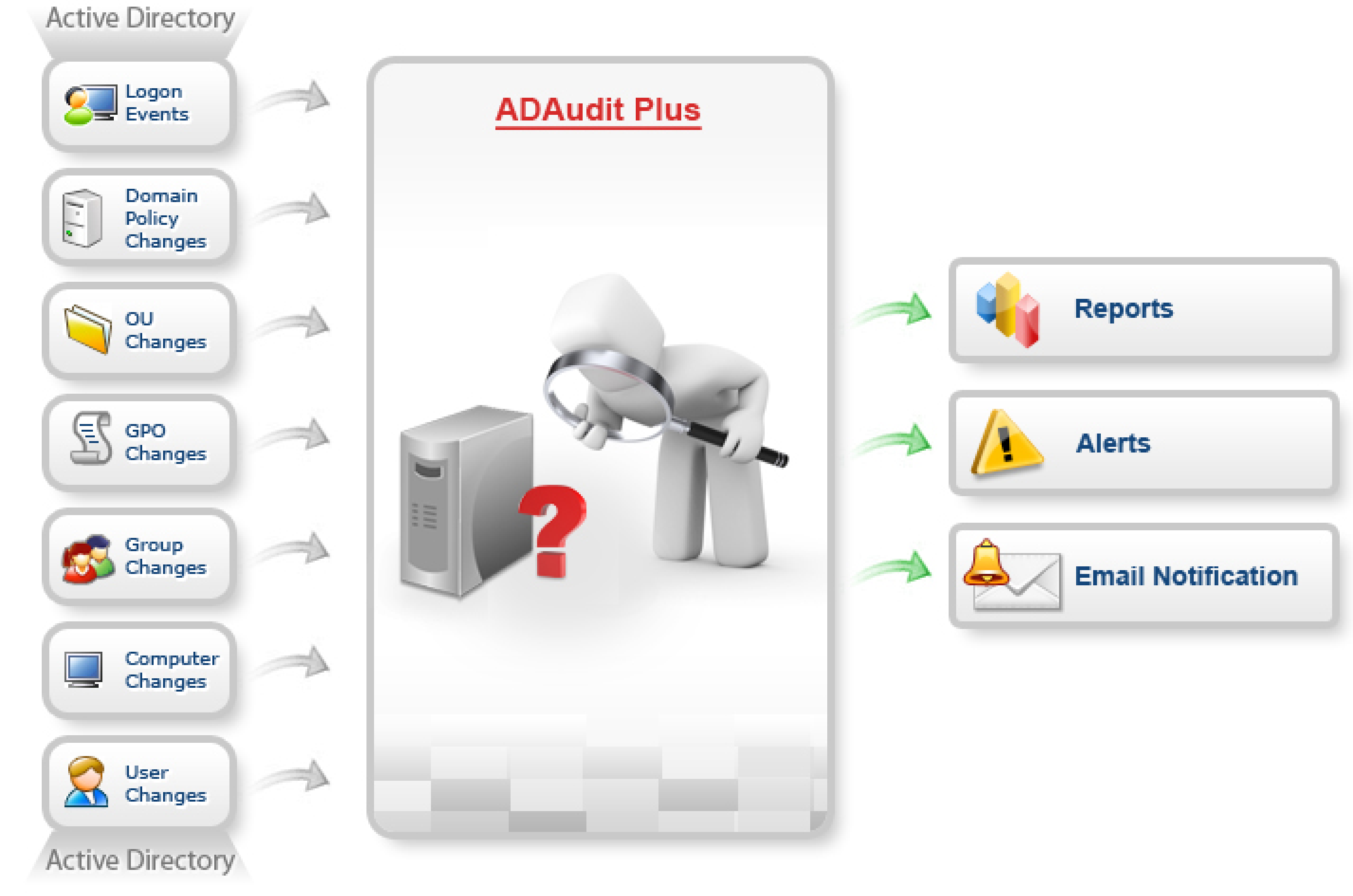
ManageEngine ADAudit Plus

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



Active Directory

Logon Events

Domain Policy Changes

OU Changes

GPO Changes

Group Changes

Computer Changes

User Changes

Active Directory

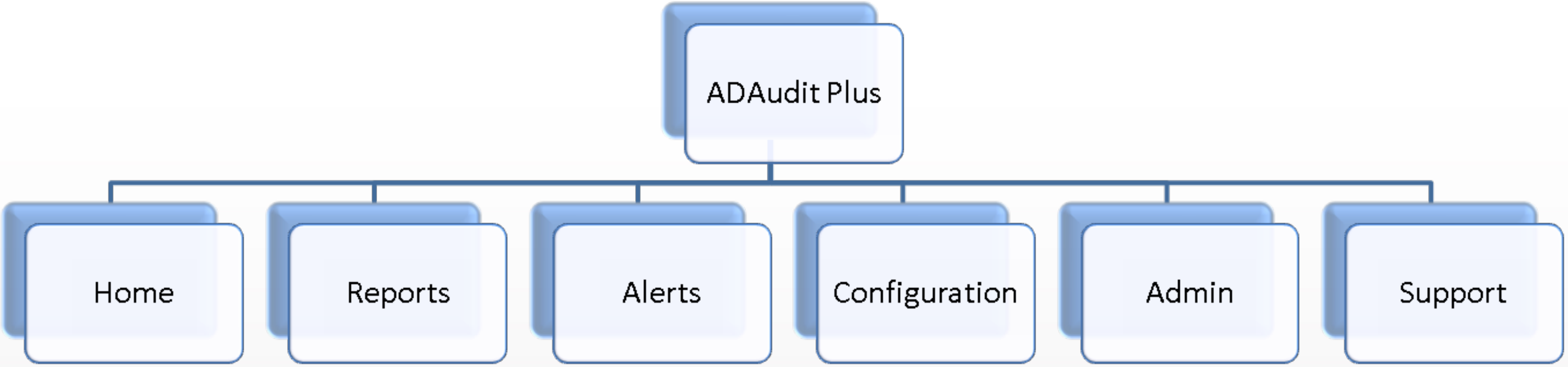
ADAudit Plus

Reports

Alerts

Email Notification

Tabs in ADAudit Plus



Home Tab of ADAudit Plus

Dashboard / 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

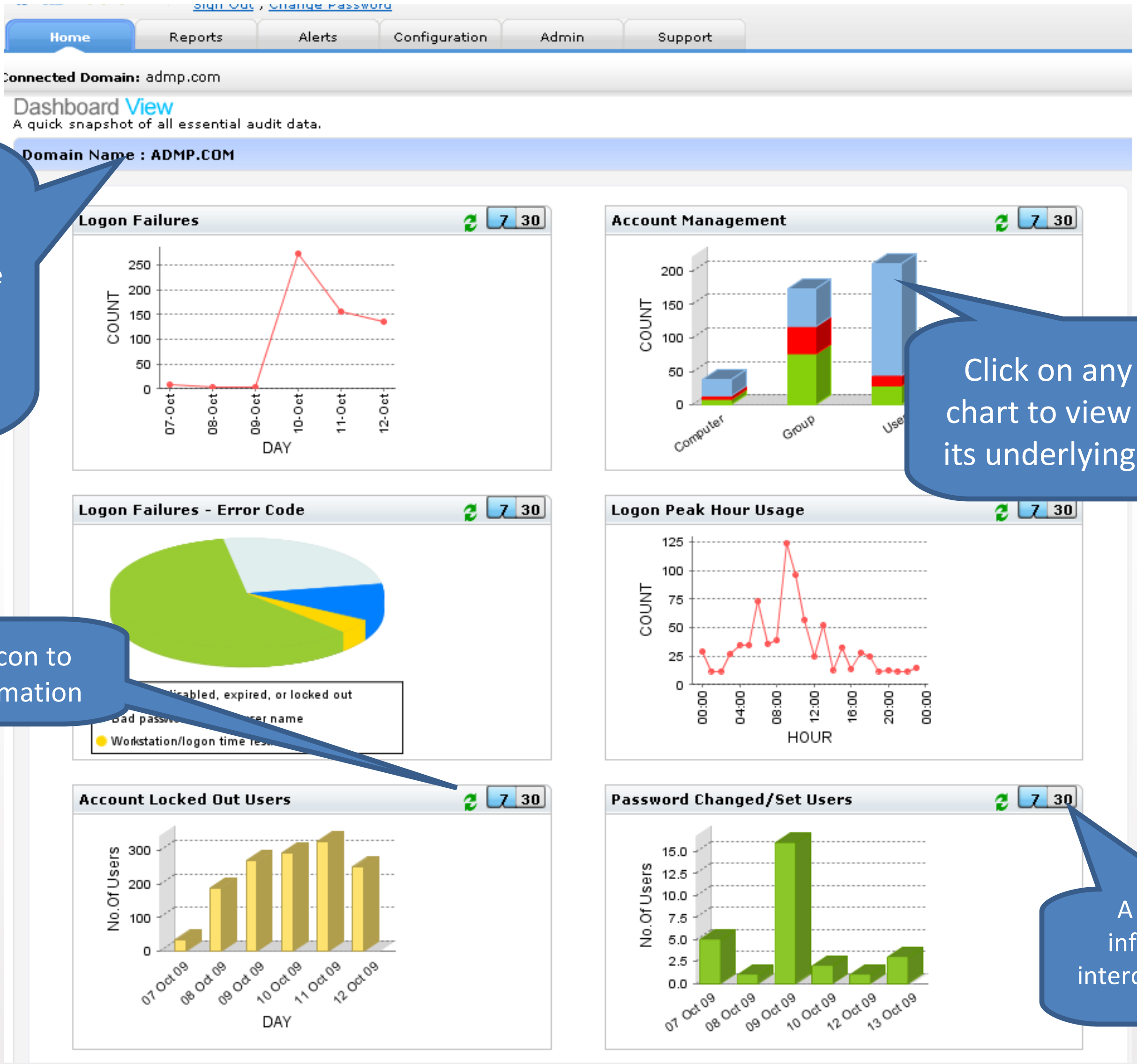
  1. Peak Logon hour of a day with the average logon count for every hour.
  2. Account (user, computer and group) management actions like created, deleted and modified all available on a single graphical interface.

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



Connected Domain: admp.com

Dashboard View

A quick snapshot of all essential audit data.

Domain Name : ADMP.COM

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

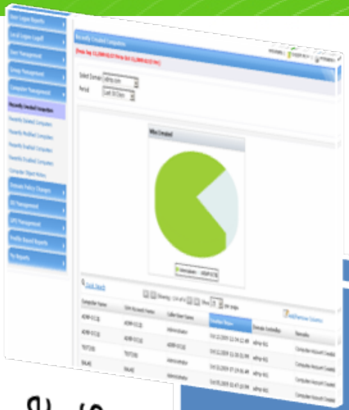
Use the refresh Icon to get updated information

A 30 day or 7 day information can be interchably selected and viewed

ADAudit Plus Reports Tab

Also explained configuration of Reports

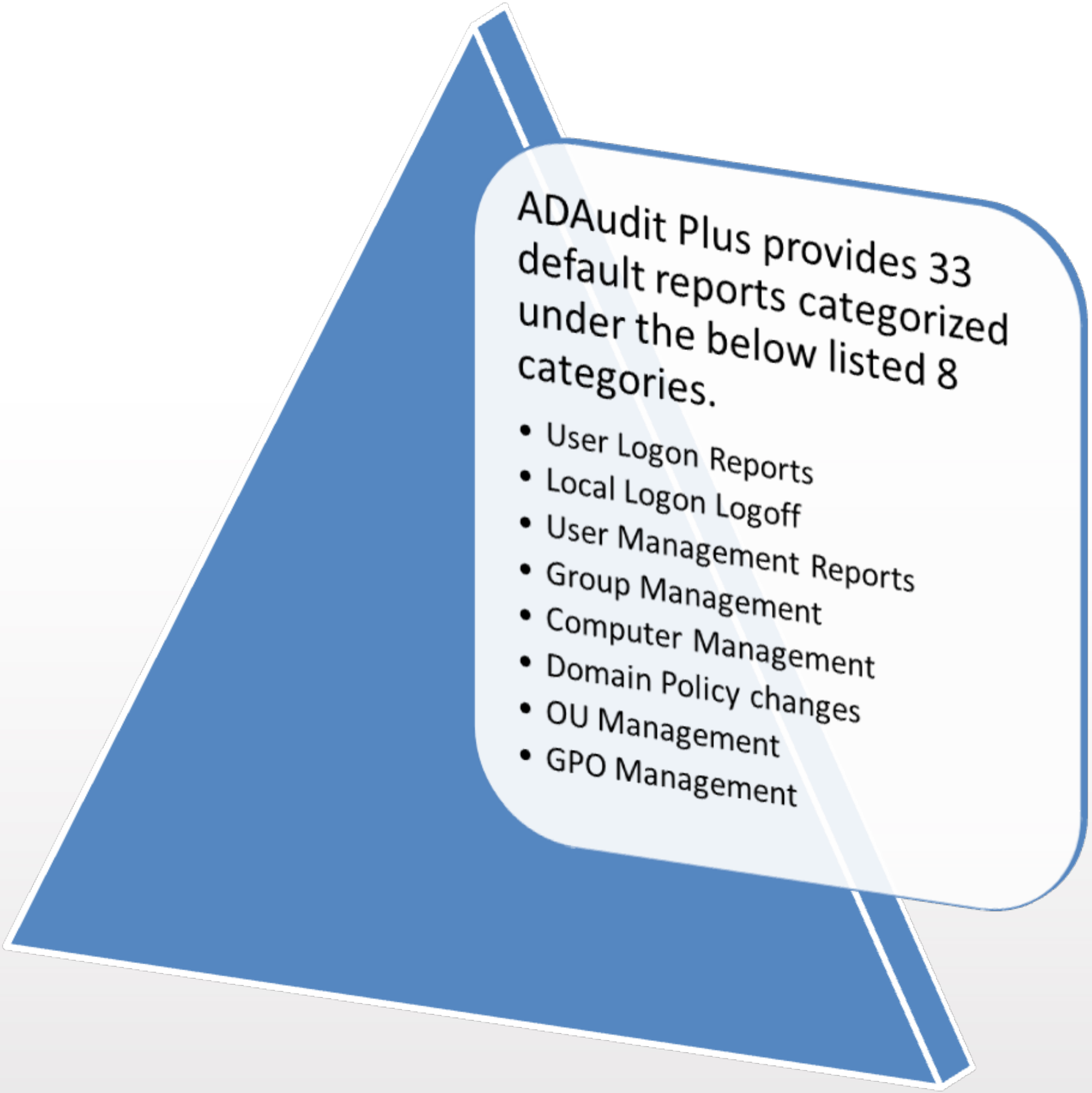
ADAudit Plus Reports



ADAudit Plus reports are provided under 3 different types

- 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.

Default Report Profile Categories



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

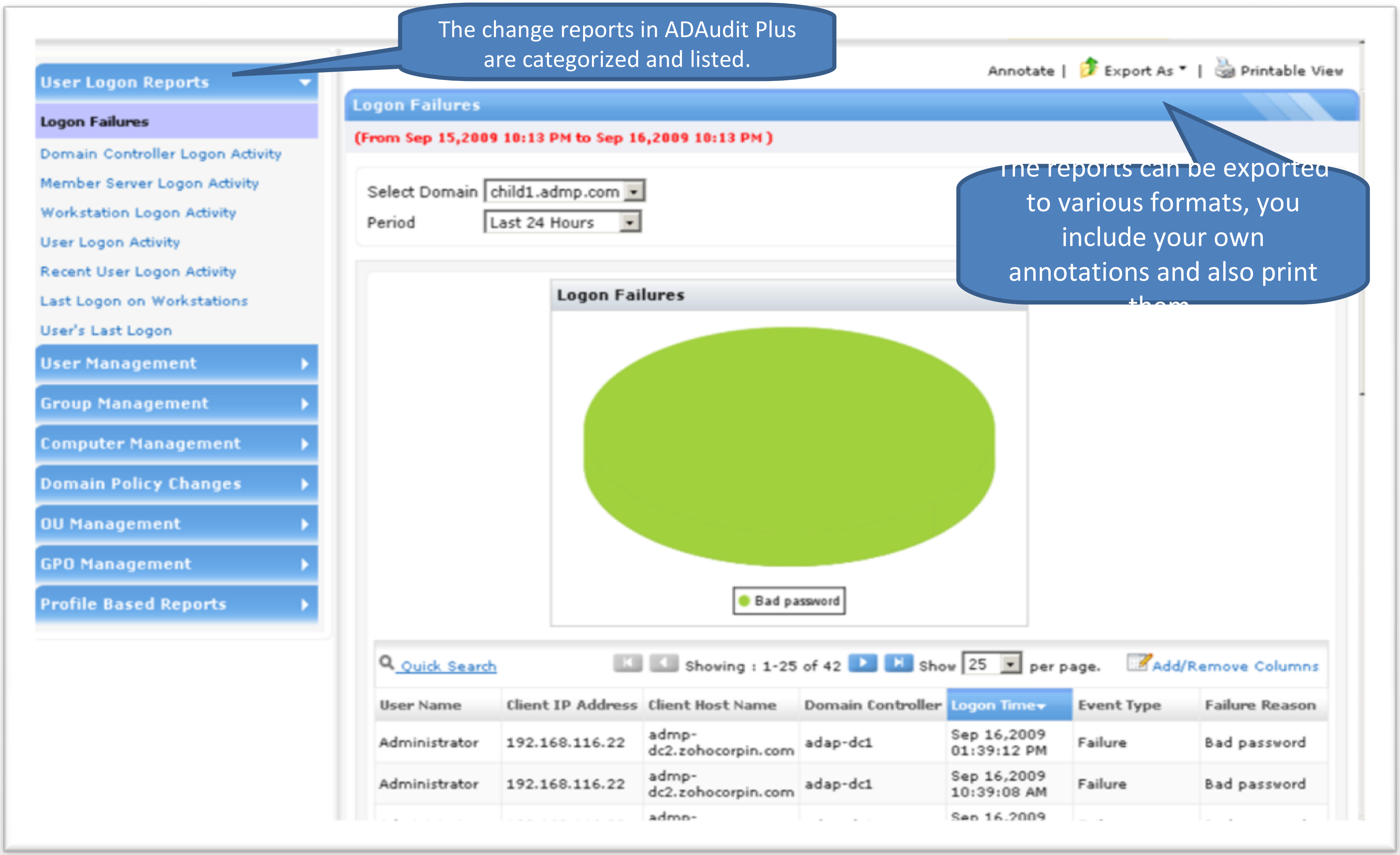
- Logon Failures
- Domain Controller Logon Activity
- Member Server Logon Activity
- Workstation Logon Activity
- User Logon Activity
- Recent User Logon Activity
- Last Logon on Workstations
- User’s Last Logon

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

Logon Failures

(From Sep 15,2009 10:13 PM to Sep 16,2009 10:13 PM)

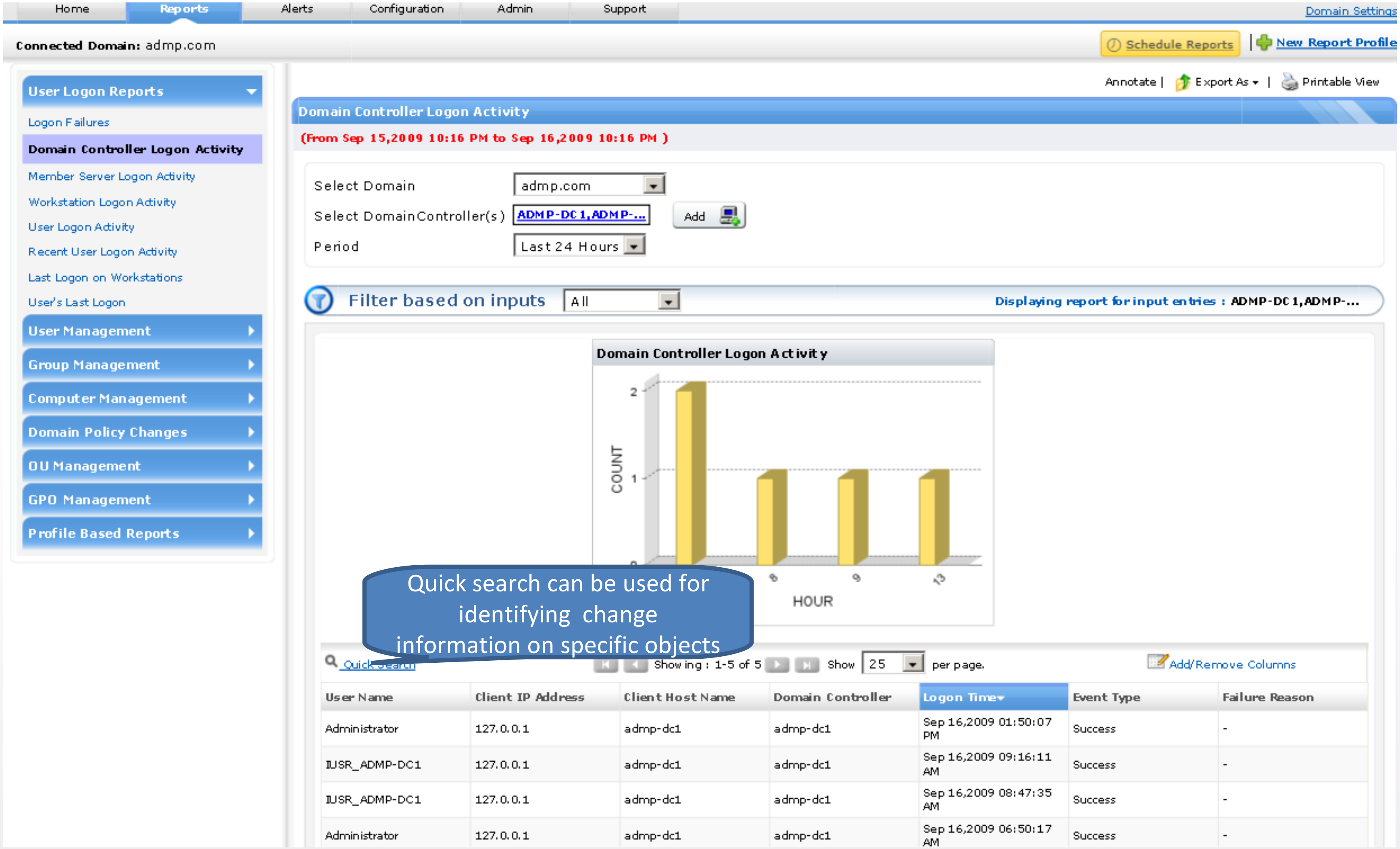
Select Domain: child1.admp.com

Period: Last 24 Hours

Showing : 1-25 of 42 Show 25 per page.

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason
Administrator	192.168.116.22	admp-dc2.zohocorpin.com	adap-dc1	Sep 16,2009 01:39:12 PM	Failure	Bad password
Administrator	192.168.116.22	admp-dc2.zohocorpin.com	adap-dc1	Sep 16,2009 10:39:08 AM	Failure	Bad password
		admp-		Sep 16,2009		

Domain Controllers Logon Activity



Connected Domain: admp.com

- 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

Domain Controller Logon Activity

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

Select Domain: admp.com

Select DomainController(s): ADMP-DC1,ADMP-...

Period: Last 24 Hours

Filter based on inputs: All

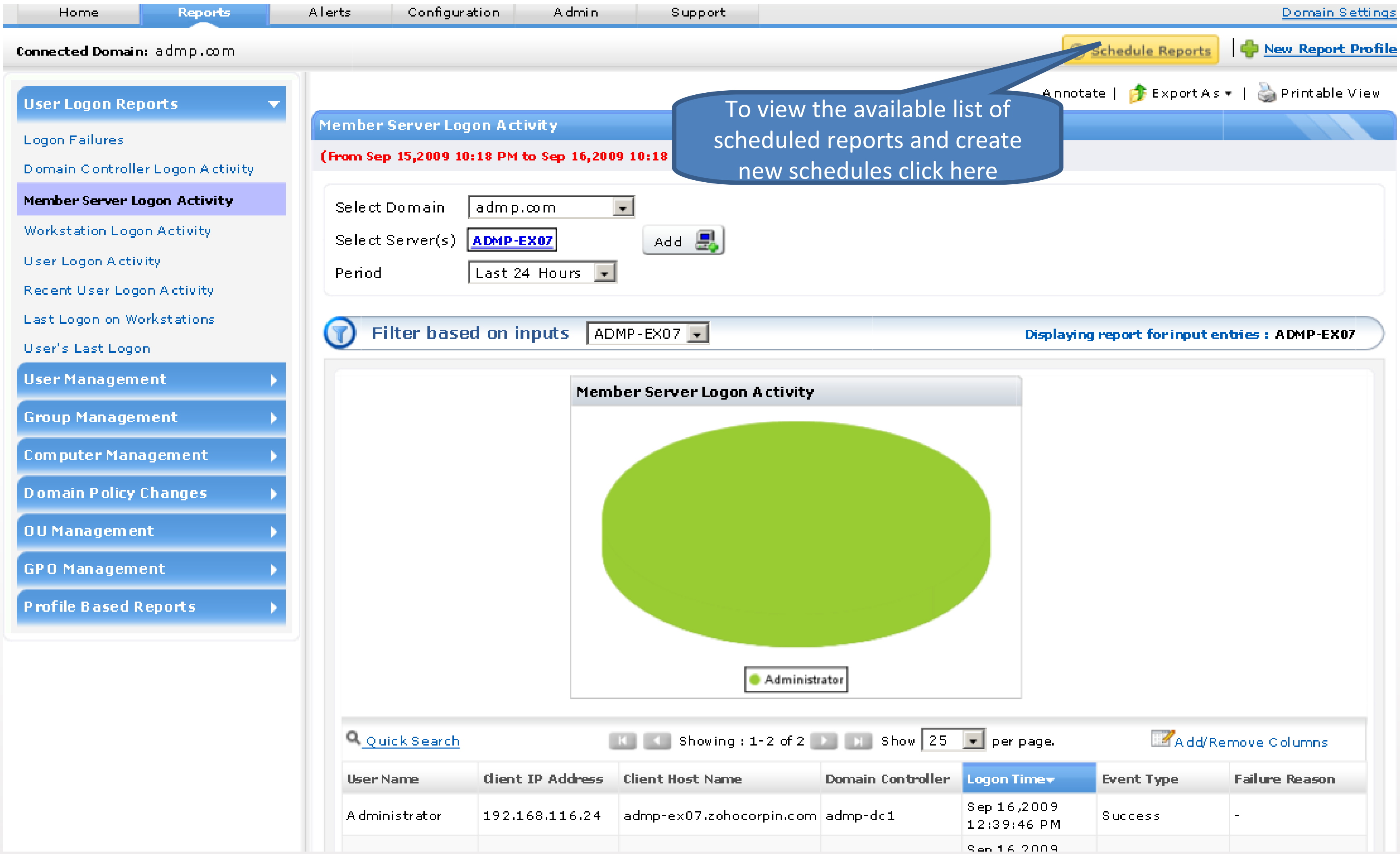
Displaying report for input entries : ADMP-DC1,ADMP-...

Showing : 1-5 of 5 Show 25 per page.

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 16,2009 01:50:07 PM	Success	-
IUSR_ADMP-DC1	127.0.0.1	admp-dc1	admp-dc1	Sep 16,2009 09:16:11 AM	Success	-
IUSR_ADMP-DC1	127.0.0.1	admp-dc1	admp-dc1	Sep 16,2009 08:47:35 AM	Success	-
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 16,2009 06:50:17 AM	Success	-

Quick search can be used for identifying change information on specific objects

Member Server Logon Activity



To view the available list of scheduled reports and create new schedules click here

Connected Domain: admp.com

Member Server Logon Activity

(From Sep 15,2009 10:18 PM to Sep 16,2009 10:18

Select Domain: admp.com

Select Server(s): ADMP-EX07

Period: Last 24 Hours

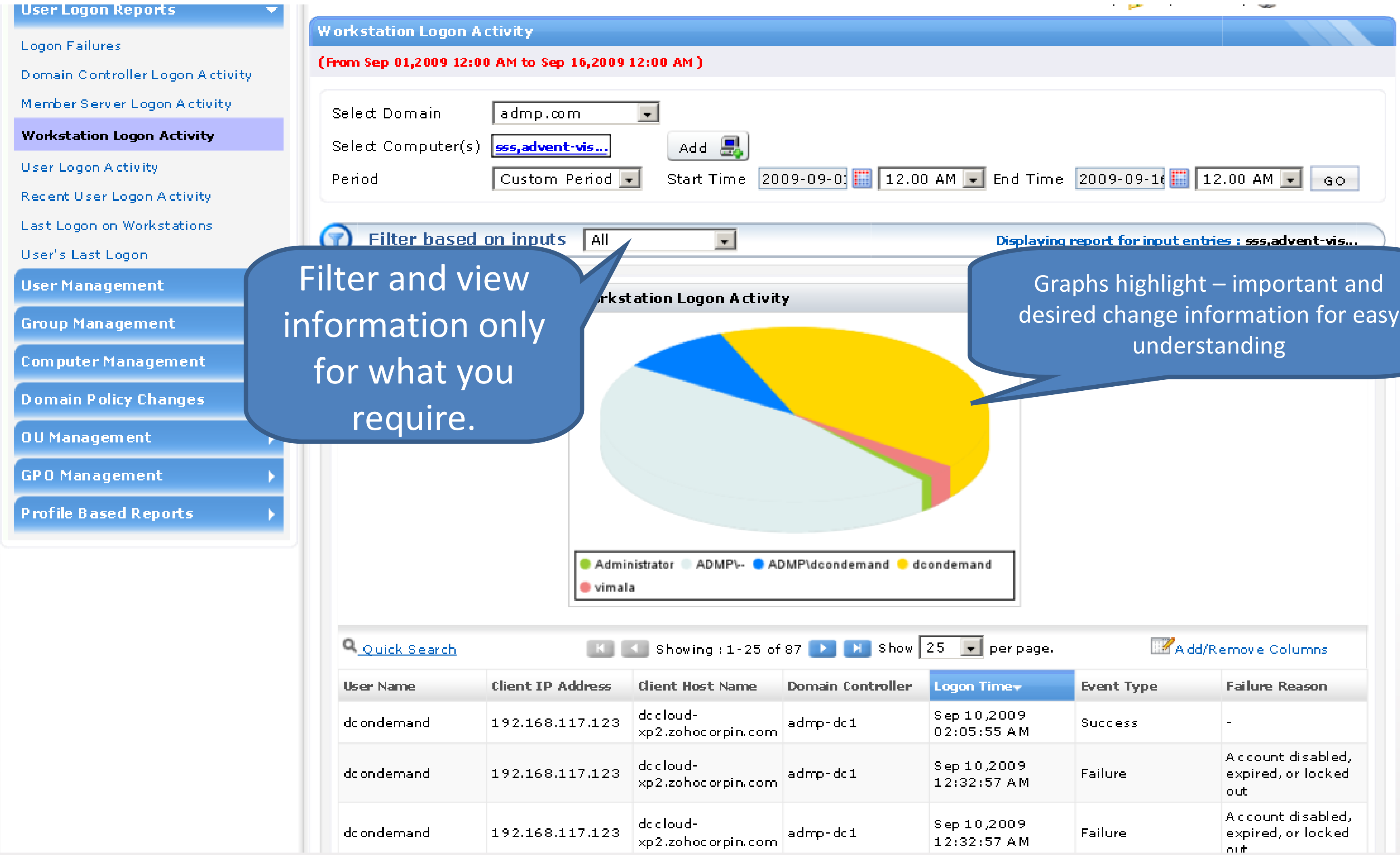
Filter based on inputs: ADMP-EX07

Displaying report for input entries : ADMP-EX07

Showing : 1-2 of 2   Show 25 per page.

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason
Administrator	192.168.116.24	admp-ex07.zohocorpin.com	admp-dc1	Sep 16,2009 12:39:46 PM	Success	-
				Sep 16,2009		

Workstation Logon Activity



Filter and view information only for what you require.

Graphs highlight – important and desired change information for easy understanding

- User Logon Reports
  - 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
- User Management
- Group Management
- Computer Management
- Domain Policy Changes
- OU Management
- GPO Management
- Profile Based Reports

Workstation Logon Activity

(From Sep 01,2009 12:00 AM to Sep 16,2009 12:00 AM)

Select Domain: admp.com

Select Computer(s): sss,advent-vis...

Period: Custom Period

Start Time: 2009-09-01 12.00 AM

End Time: 2009-09-16 12.00 AM

Filter based on inputs: All

Displaying report for input entries : sss,advent-vis...

Workstation Logon Activity

● Administrator ● ADMP\- ● ADMP\dcondemand ● dcondemand ● vimala

Quick Search

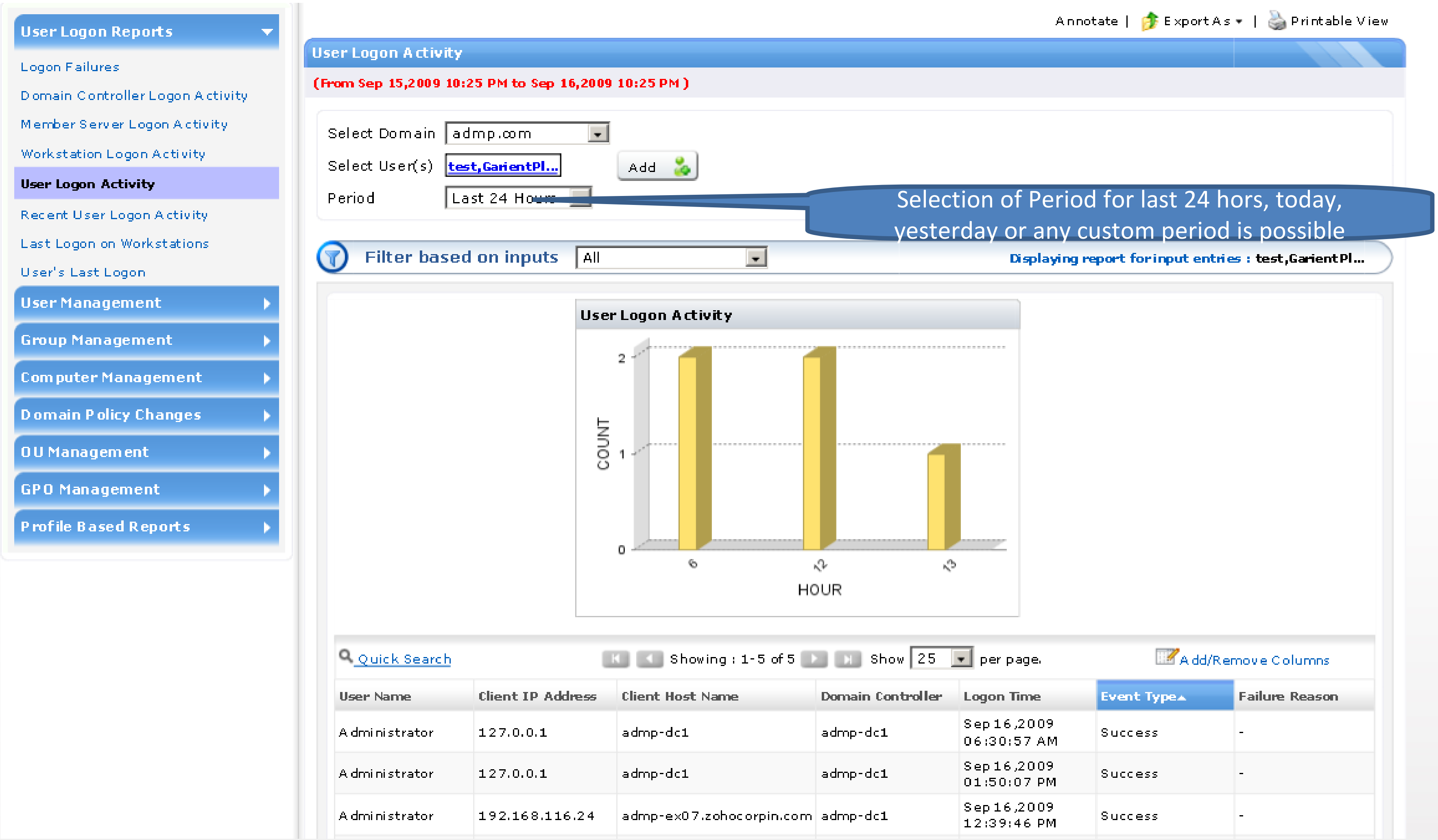
Showing : 1-25 of 87

Show 25 per page.

Add/Remove Columns

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason
dcondemand	192.168.117.123	dccloud-xp2.zohocorpin.com	admp-dc1	Sep 10,2009 02:05:55 AM	Success	-
dcondemand	192.168.117.123	dccloud-xp2.zohocorpin.com	admp-dc1	Sep 10,2009 12:32:57 AM	Failure	Account disabled, expired, or locked out
dcondemand	192.168.117.123	dccloud-xp2.zohocorpin.com	admp-dc1	Sep 10,2009 12:32:57 AM	Failure	Account disabled, expired, or locked out

User Logon Activity



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,GarientPl...

Add

Period: Last 24 Hours

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

Filter based on inputs: All

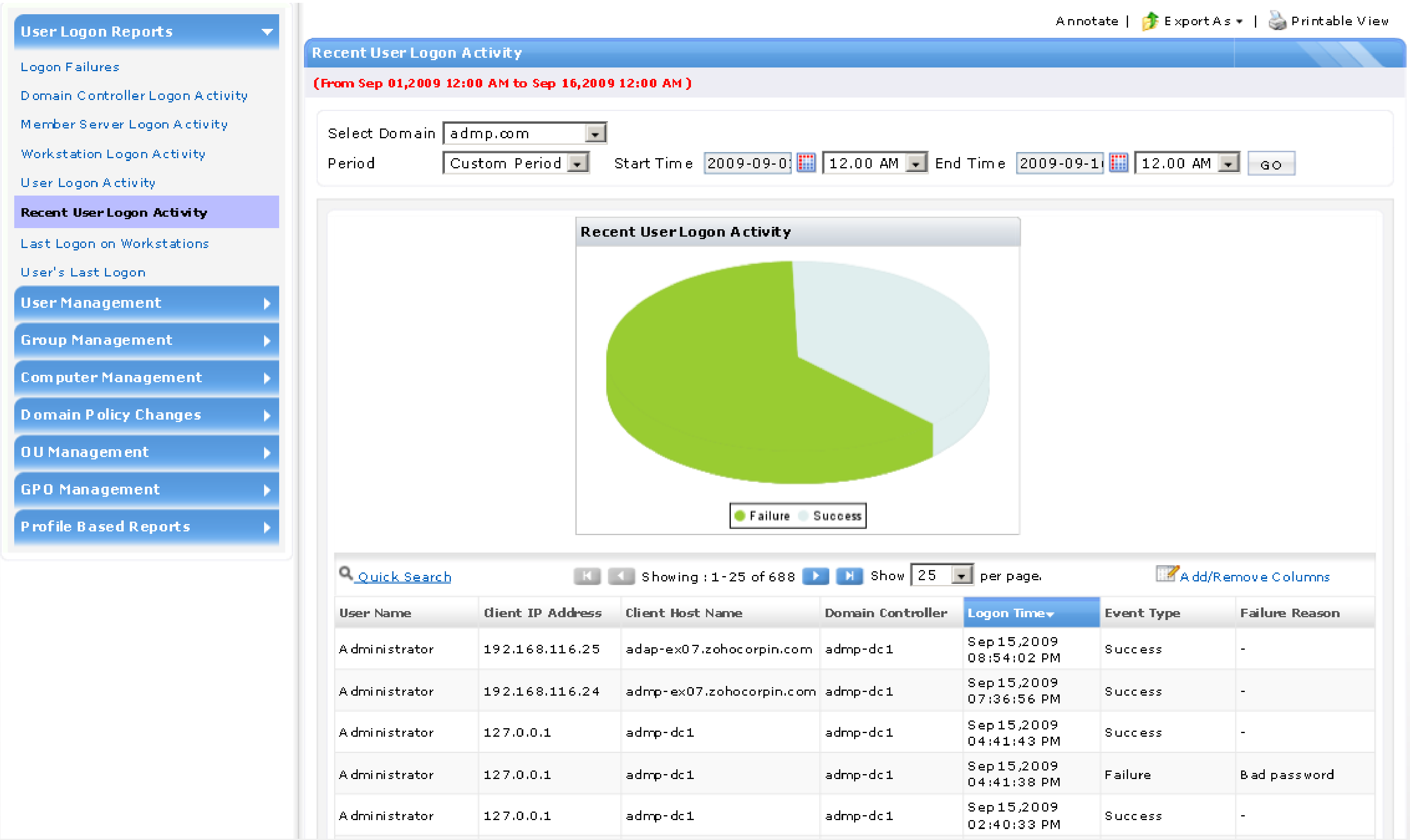
Displaying report for input entries : test,GarientPl...

User Logon Activity

Quick Search | Showing : 1-5 of 5 | Show 25 per page. | Add/Remove Columns

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 16,2009 06:30:57 AM	Success	-
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 16,2009 01:50:07 PM	Success	-
Administrator	192.168.116.24	admp-ex07.zohocorpin.com	admp-dc1	Sep 16,2009 12:39:46 PM	Success	-

Recent User Logon Activity- Status



Recent User Logon Activity

(From Sep 01,2009 12:00 AM to Sep 16,2009 12:00 AM)

Select Domain: admp.com

Period: Custom Period

Start Time: 2009-09-0 12.00 AM

End Time: 2009-09-1 12.00 AM

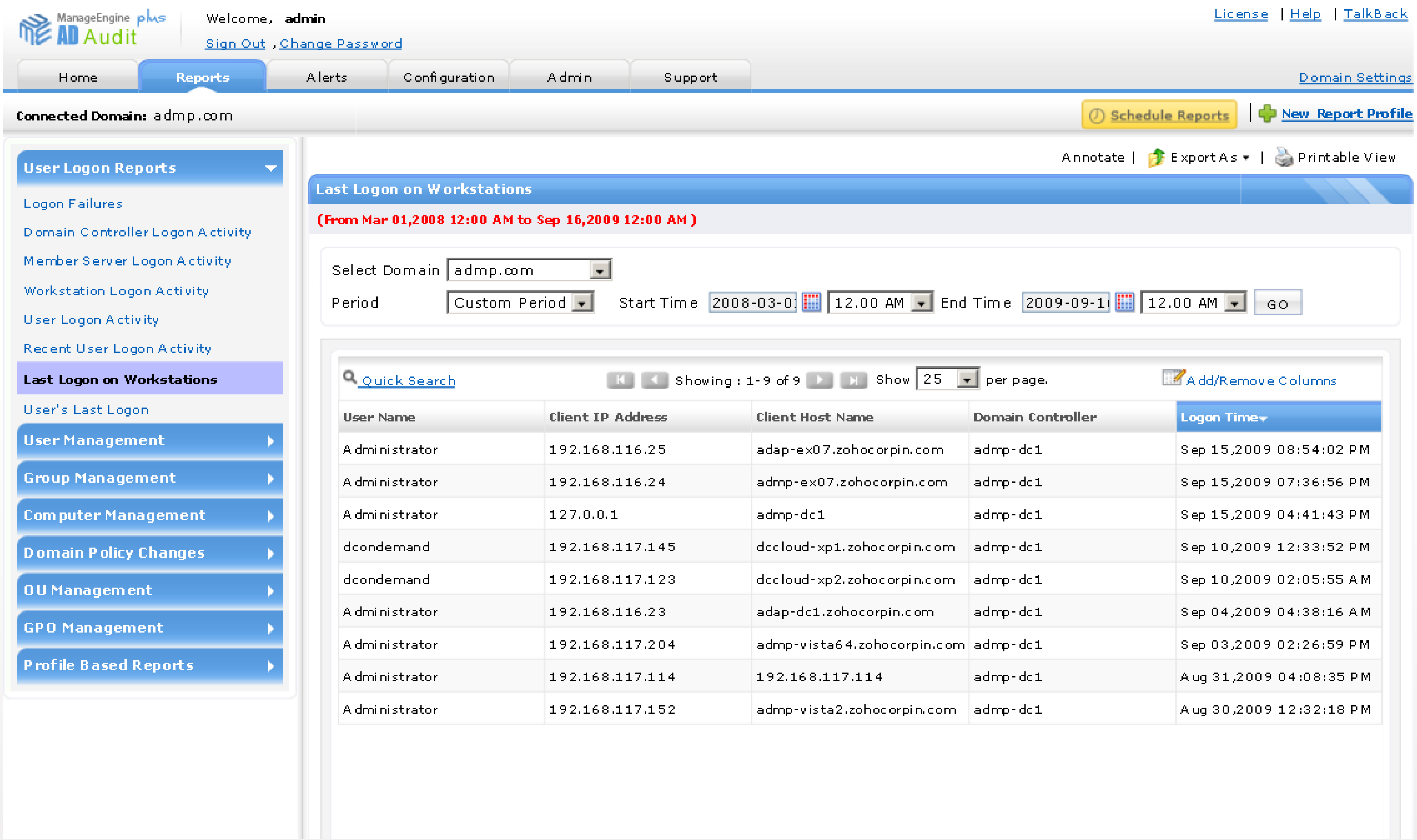
Recent User Logon Activity

Showing : 1-25 of 688

Show 25 per page.

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason
Administrator	192.168.116.25	adap-ex07.zohocorpin.com	admp-dc1	Sep 15,2009 08:54:02 PM	Success	-
Administrator	192.168.116.24	admp-ex07.zohocorpin.com	admp-dc1	Sep 15,2009 07:36:56 PM	Success	-
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 15,2009 04:41:43 PM	Success	-
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 15,2009 04:41:38 PM	Failure	Bad password
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 15,2009 02:40:33 PM	Success	-

Last Logon on Workstation – User’s last login info



Connected Domain: admp.com

Last Logon on Workstations

(From Mar 01,2008 12:00 AM to Sep 16,2009 12:00 AM)

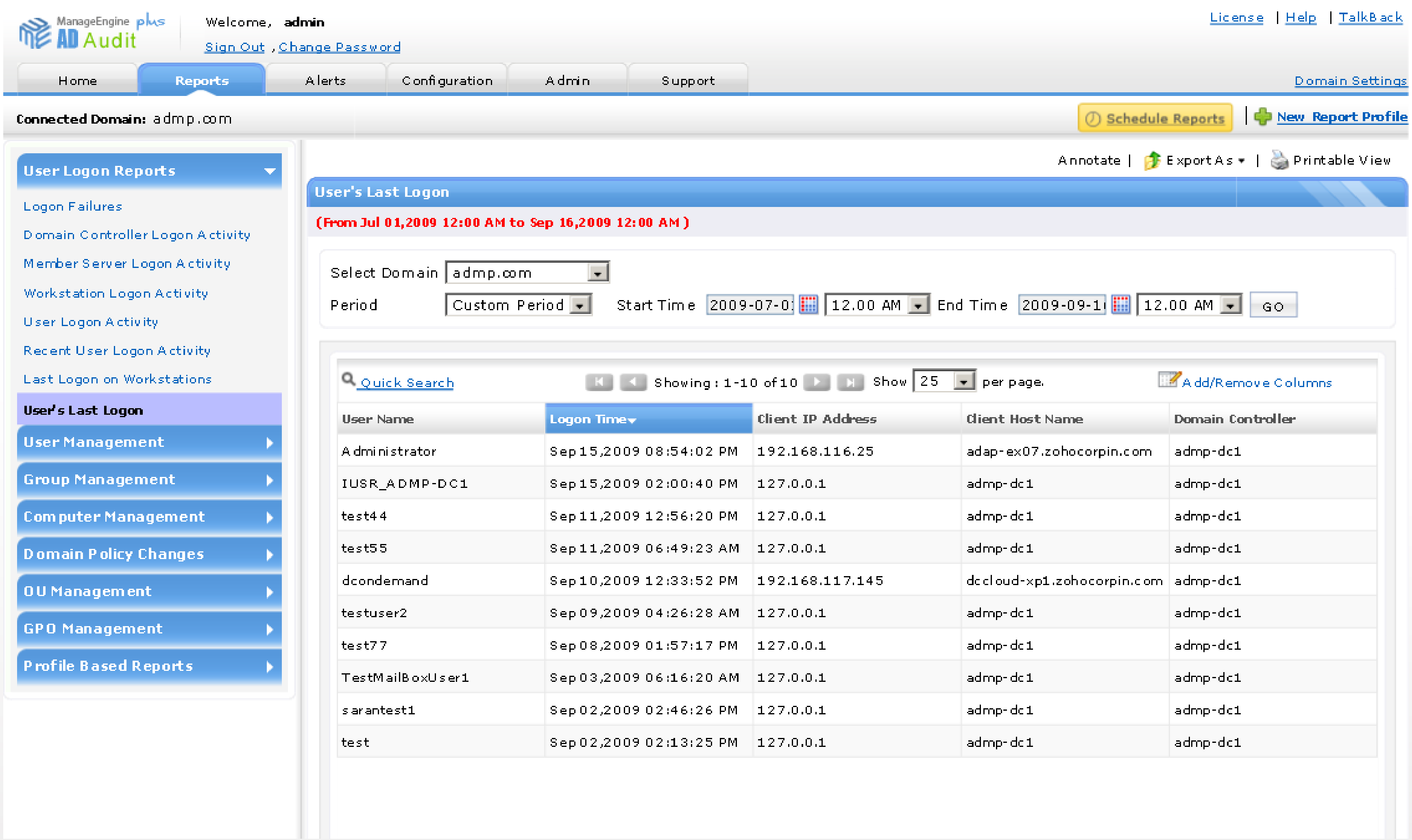
Select Domain: admp.com

Period: Custom Period Start Time: 2008-03-01 12.00 AM End Time: 2009-09-1 12.00 AM

Showing : 1-9 of 9 Show 25 per page.

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time
Administrator	192.168.116.25	adap-ex07.zohocorpin.com	admp-dc1	Sep 15,2009 08:54:02 PM
Administrator	192.168.116.24	admp-ex07.zohocorpin.com	admp-dc1	Sep 15,2009 07:36:56 PM
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 15,2009 04:41:43 PM
dcondemand	192.168.117.145	dccloud-xp1.zohocorpin.com	admp-dc1	Sep 10,2009 12:33:52 PM
dcondemand	192.168.117.123	dccloud-xp2.zohocorpin.com	admp-dc1	Sep 10,2009 02:05:55 AM
Administrator	192.168.116.23	adap-dc1.zohocorpin.com	admp-dc1	Sep 04,2009 04:38:16 AM
Administrator	192.168.117.204	admp-vista64.zohocorpin.com	admp-dc1	Sep 03,2009 02:26:59 PM
Administrator	192.168.117.114	192.168.117.114	admp-dc1	Aug 31,2009 04:08:35 PM
Administrator	192.168.117.152	admp-vista2.zohocorpin.com	admp-dc1	Aug 30,2009 12:32:18 PM

User’s Last Logon – computer info.



Connected Domain: admp.com

User's Last Logon

(From Jul 01,2009 12:00 AM to Sep 16,2009 12:00 AM)

Select Domain: admp.com

Period: Custom Period   Start Time: 2009-07-01 12.00 AM   End Time: 2009-09-1 12.00 AM

Showing : 1-10 of 10   Show 25 per page.

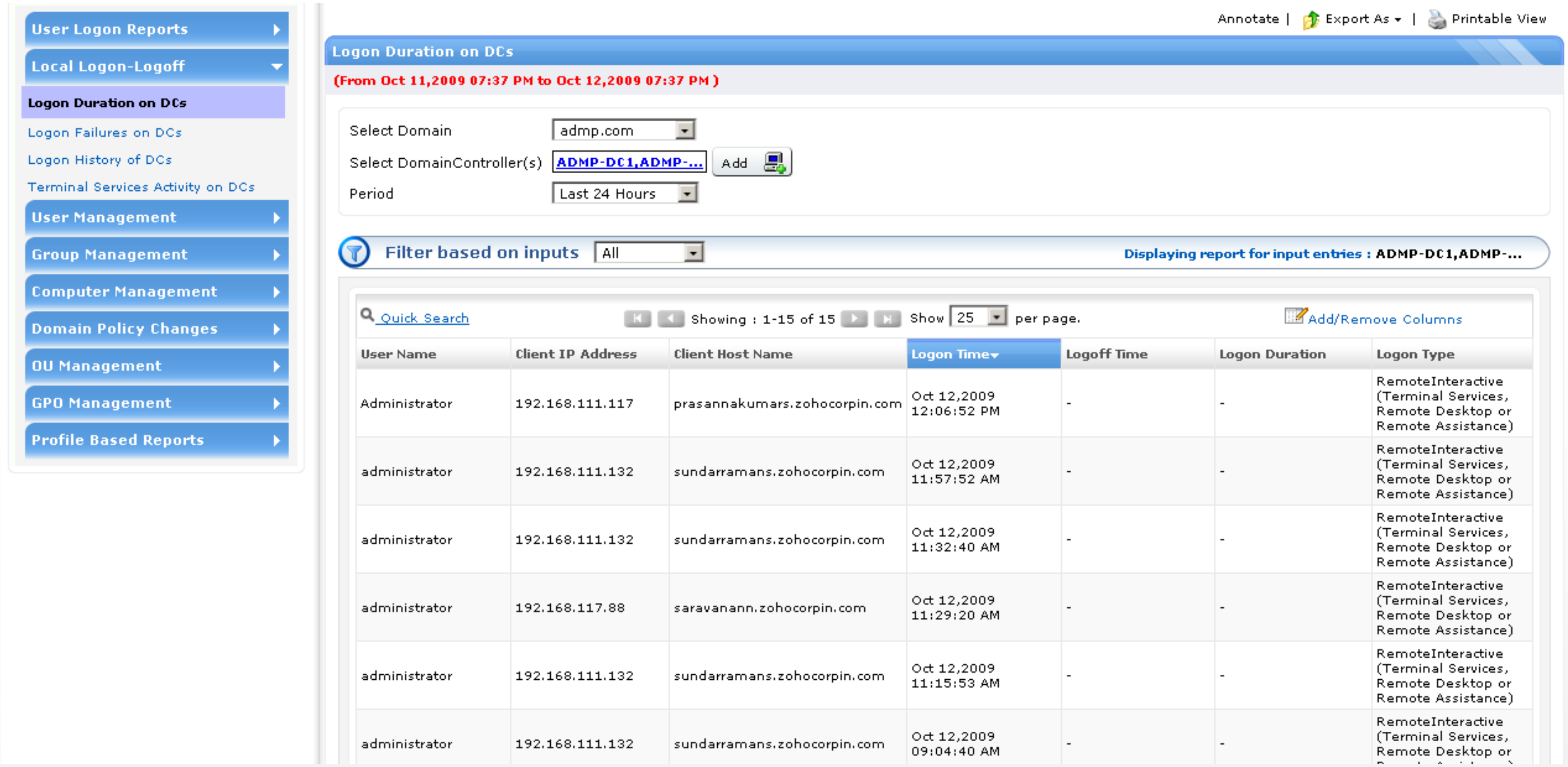
User Name	Logon Time	Client IP Address	Client Host Name	Domain Controller
Administrator	Sep 15,2009 08:54:02 PM	192.168.116.25	adap-ex07.zohocorpin.com	admp-dc1
IUSR_ADMP-DC1	Sep 15,2009 02:00:40 PM	127.0.0.1	admp-dc1	admp-dc1
test44	Sep 11,2009 12:56:20 PM	127.0.0.1	admp-dc1	admp-dc1
test55	Sep 11,2009 06:49:23 AM	127.0.0.1	admp-dc1	admp-dc1
dcondemand	Sep 10,2009 12:33:52 PM	192.168.117.145	dccloud-xp1.zohocorpin.com	admp-dc1
testuser2	Sep 09,2009 04:26:28 AM	127.0.0.1	admp-dc1	admp-dc1
test77	Sep 08,2009 01:57:17 PM	127.0.0.1	admp-dc1	admp-dc1
TestMailBoxUser1	Sep 03,2009 06:16:20 AM	127.0.0.1	admp-dc1	admp-dc1
sarantest1	Sep 02,2009 02:46:26 PM	127.0.0.1	admp-dc1	admp-dc1
test	Sep 02,2009 02:13:25 PM	127.0.0.1	admp-dc1	admp-dc1

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 Duration on Domain Controllers



Logon Duration on DCs

(From Oct 11,2009 07:37 PM to Oct 12,2009 07:37 PM)

Select Domain: admp.com

Select DomainController(s): ADMP-DC1,ADMP-...

Period: Last 24 Hours

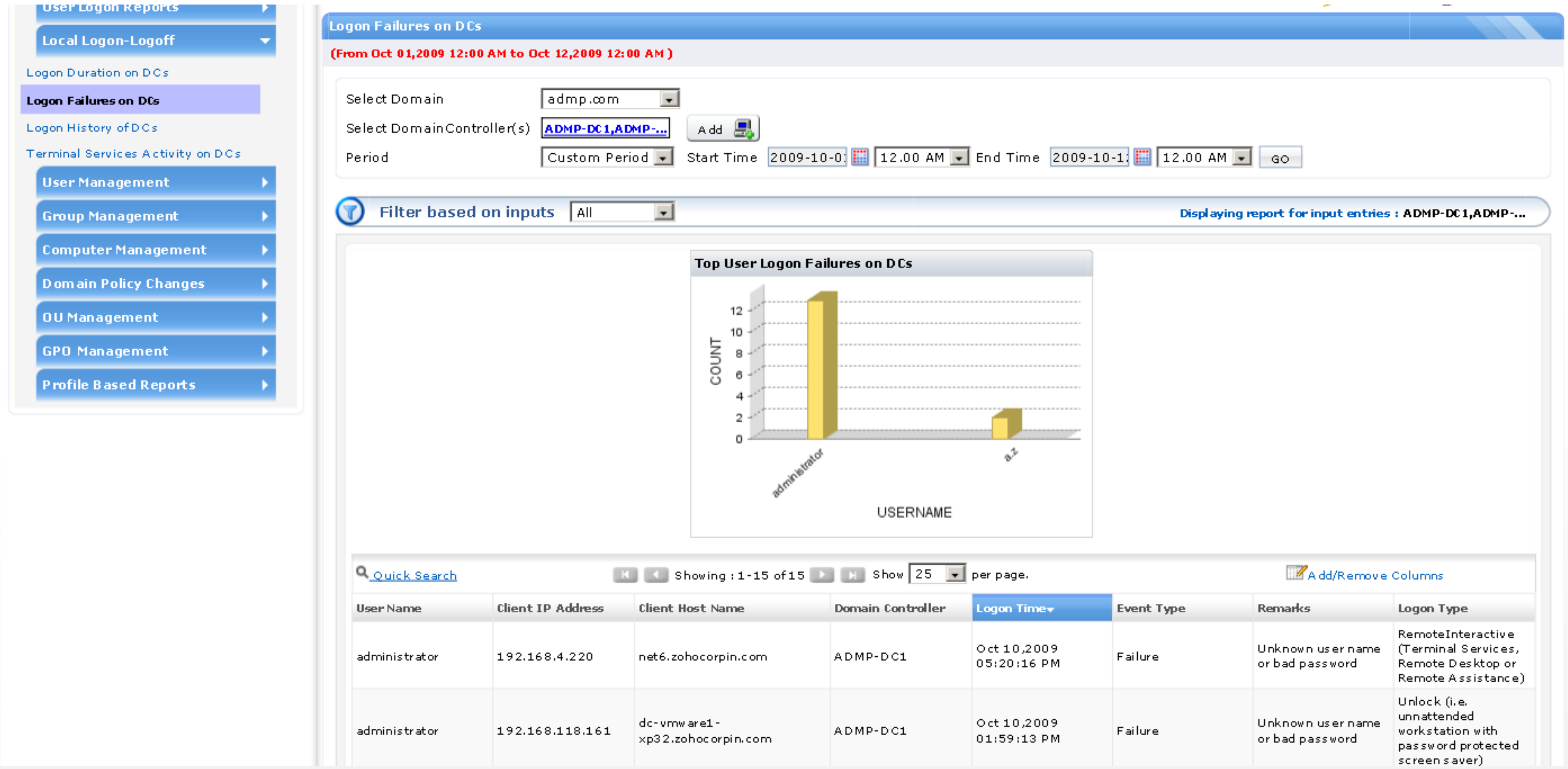
Filter based on inputs: All

Displaying report for input entries : ADMP-DC1,ADMP-...

Showing : 1-15 of 15 Show 25 per page.

User Name	Client IP Address	Client Host Name	Logon Time	Logoff Time	Logon Duration	Logon Type
Administrator	192.168.111.117	prasannakumars.zohocorpin.com	Oct 12,2009 12:06:52 PM	-	-	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	192.168.111.132	sundarramans.zohocorpin.com	Oct 12,2009 11:57:52 AM	-	-	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	192.168.111.132	sundarramans.zohocorpin.com	Oct 12,2009 11:32:40 AM	-	-	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	192.168.117.88	saravanann.zohocorpin.com	Oct 12,2009 11:29:20 AM	-	-	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	192.168.111.132	sundarramans.zohocorpin.com	Oct 12,2009 11:15:53 AM	-	-	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	192.168.111.132	sundarramans.zohocorpin.com	Oct 12,2009 09:04:40 AM	-	-	RemoteInteractive (Terminal Services, Remote Desktop or

Logon Failure on DCs



Logon Failures on DCs

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

Select Domain: admp.com

Select DomainController(s): ADMP-DC1,ADMP-... Add

Period: Custom Period | Start Time: 2009-10-0: 12.00 AM | End Time: 2009-10-1: 12.00 AM | GO

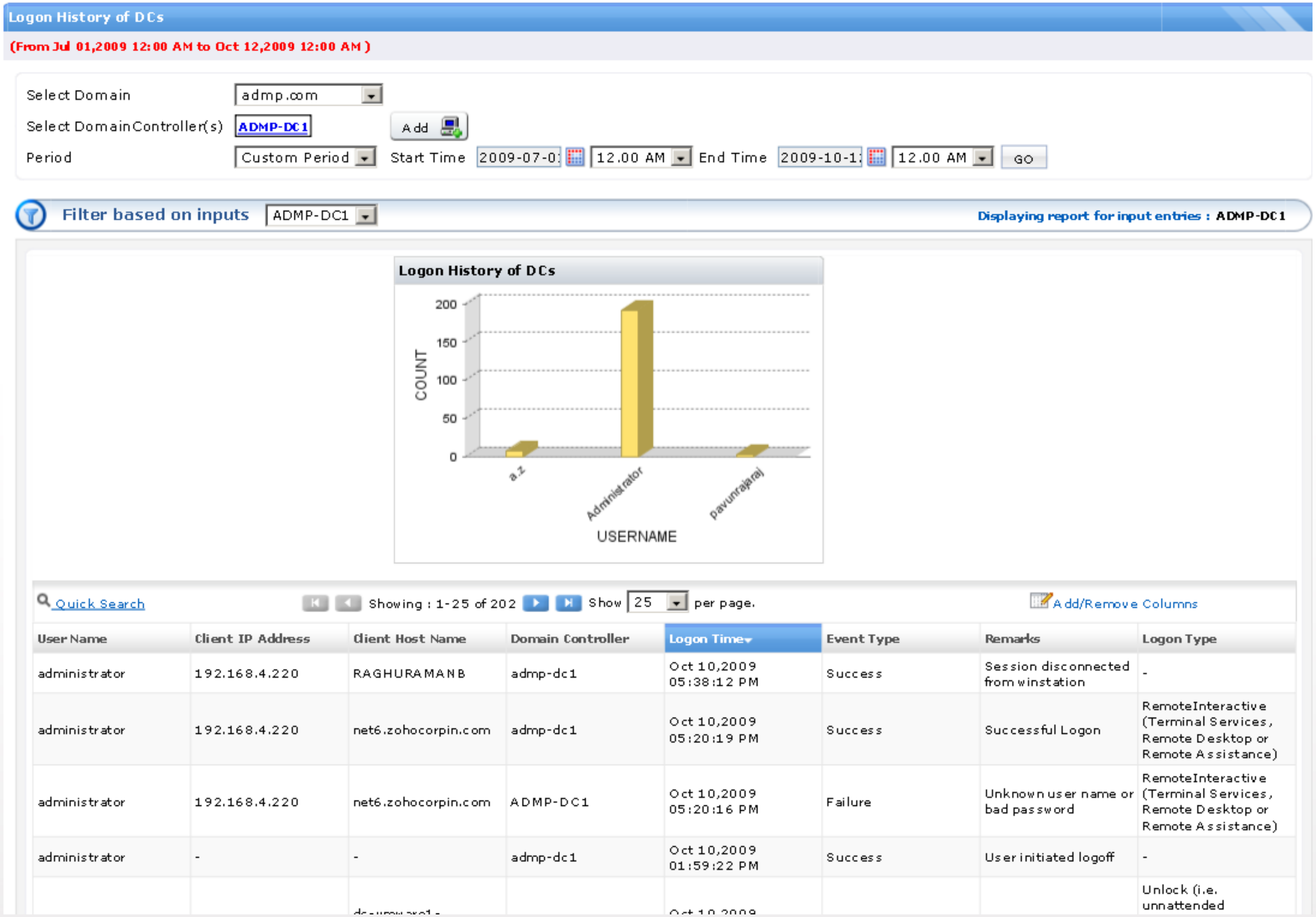
Filter based on inputs: All

Displaying report for input entries : ADMP-DC1,ADMP-...

Quick Search | Showing : 1-15 of 15 | Show 25 per page. | Add/Remove Columns

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Remarks	Logon Type
administrator	192.168.4.220	net6.zohocorpin.com	ADMP-DC1	Oct 10,2009 05:20:16 PM	Failure	Unknown user name or bad password	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	192.168.118.161	dc-vmware1-xp32.zohocorpin.com	ADMP-DC1	Oct 10,2009 01:59:13 PM	Failure	Unknown user name or bad password	Unlock (i.e. unattended workstation with password protected screen saver)

Logon History of DCs



Logon History of DCs

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

Select Domain: admp.com

Select DomainController(s): ADMP-DC1

Period: Custom Period — Start Time 2009-07-0 12.00 AM — End Time 2009-10-1 12.00 AM

Filter based on inputs: ADMP-DC1

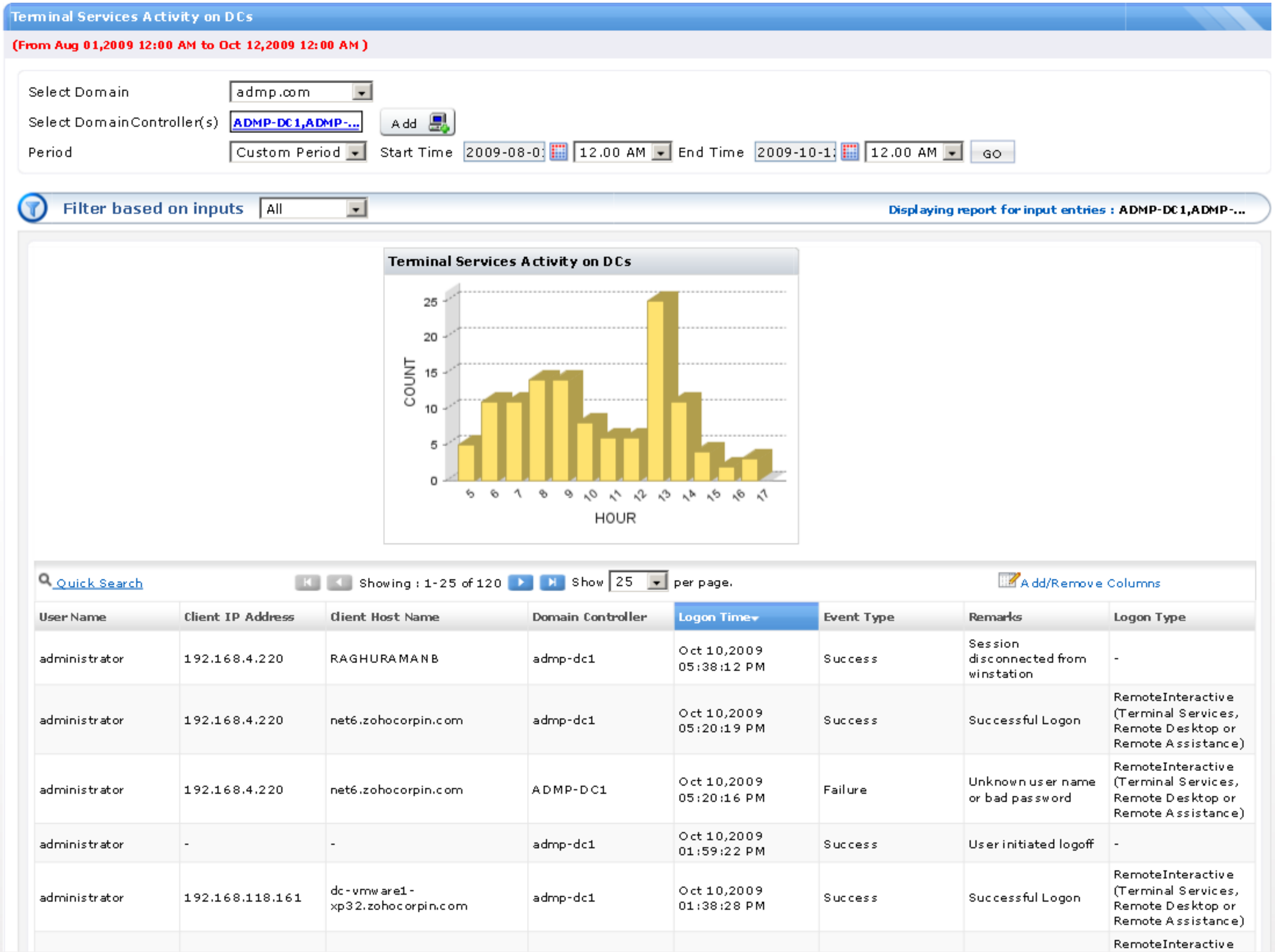
Displaying report for input entries : ADMP-DC1

Logon History of DCs

Showing : 1-25 of 202 Show 25 per page.

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Remarks	Logon Type
administrator	192.168.4.220	RAGHURAMANB	admp-dc1	Oct 10,2009 05:38:12 PM	Success	Session disconnected from winstation	-
administrator	192.168.4.220	net6.zohocorpin.com	admp-dc1	Oct 10,2009 05:20:19 PM	Success	Successful Logon	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	192.168.4.220	net6.zohocorpin.com	ADMP-DC1	Oct 10,2009 05:20:16 PM	Failure	Unknown user name or bad password	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	-	-	admp-dc1	Oct 10,2009 01:59:22 PM	Success	User initiated logoff	-
		dc-vmware1-		Oct 10,2009			Unlock (i.e. unattended

Terminal Services Activity on DCs



Terminal Services Activity on DCs

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

Select Domain	admp.com
Select DomainController(s)	ADMP-DC1,ADMP-... Add
Period	Custom Period Start Time 2009-08-0: 12.00 AM End Time 2009-10-1: 12.00 AM GO

Filter based on inputs All

Displaying report for input entries : ADMP-DC1,ADMP-...

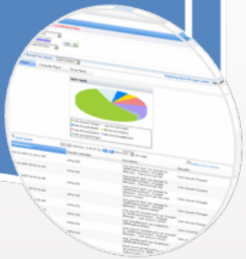
Quick Search Showing : 1-25 of 120 Show 25 per page. Add/Remove Columns

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Remarks	Logon Type
administrator	192.168.4.220	RAGHURAMANB	admp-dc1	Oct 10,2009 05:38:12 PM	Success	Session disconnected from winstation	-
administrator	192.168.4.220	net6.zohocorpin.com	admp-dc1	Oct 10,2009 05:20:19 PM	Success	Successful Logon	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	192.168.4.220	net6.zohocorpin.com	ADMP-DC1	Oct 10,2009 05:20:16 PM	Failure	Unknown user name or bad password	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
administrator	-	-	admp-dc1	Oct 10,2009 01:59:22 PM	Success	User initiated logoff	-
administrator	192.168.118.161	dc-vmware1-xp32.zohocorpin.com	admp-dc1	Oct 10,2009 01:38:28 PM	Success	Successful Logon	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
							RemoteInteractive

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.



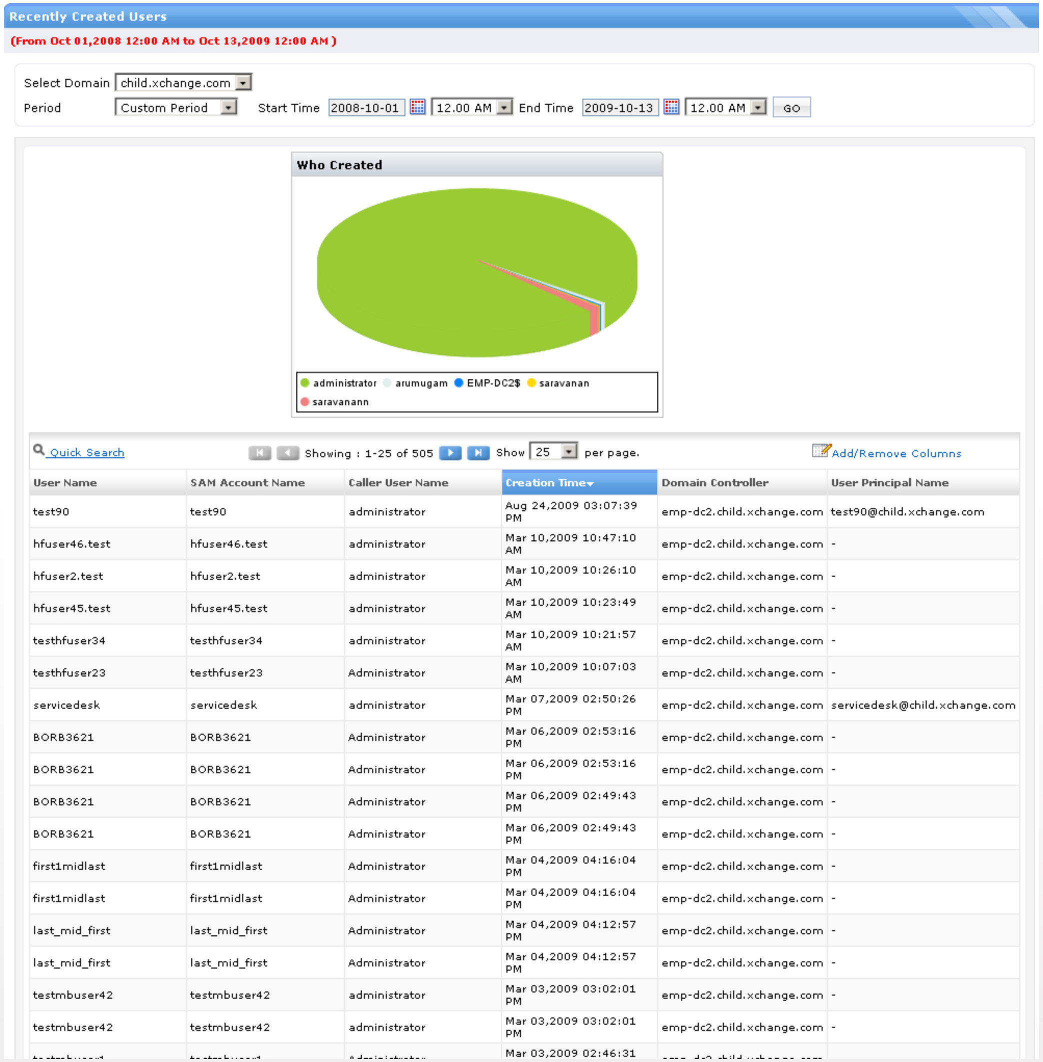
- Recently Password Changed Users
- Recently Password Set Users
- Password Never Expires Set Users
- Last Modification on Users
- Administrative User Actions
- User Object History

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



Recently Created Users

(From Oct 01,2008 12:00 AM to Oct 13,2009 12:00 AM)

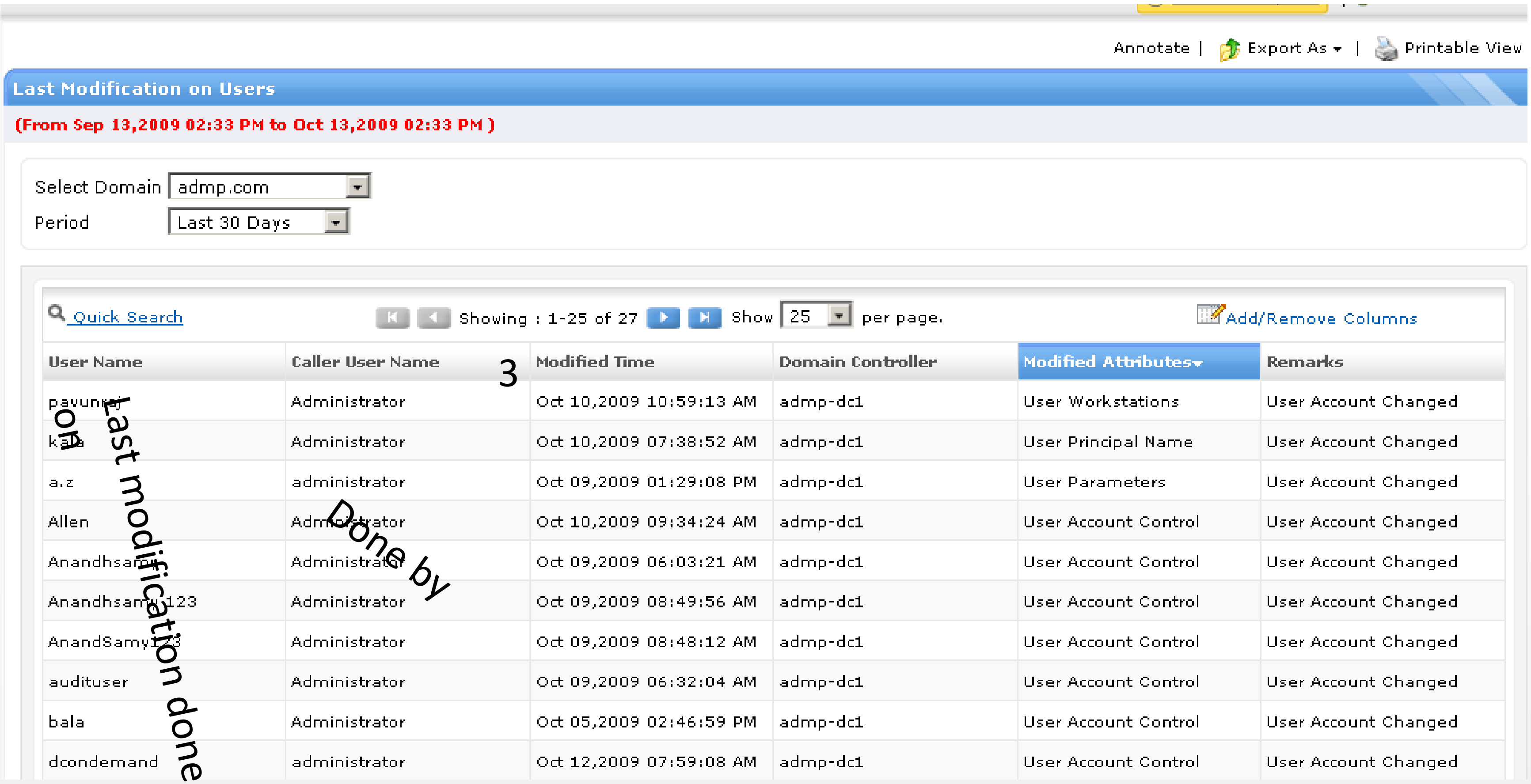
Select Domain: child.xchange.com

Period: Custom Period Start Time: 2008-10-01 12.00 AM End Time: 2009-10-13 12.00 AM GO

Who Created

User Name	SAM Account Name	Caller User Name	Creation Time	Domain Controller	User Principal Name
test90	test90	administrator	Aug 24,2009 03:07:39 PM	emp-dc2.child.xchange.com	test90@child.xchange.com
hfuser46.test	hfuser46.test	administrator	Mar 10,2009 10:47:10 AM	emp-dc2.child.xchange.com	-
hfuser2.test	hfuser2.test	administrator	Mar 10,2009 10:26:10 AM	emp-dc2.child.xchange.com	-
hfuser45.test	hfuser45.test	administrator	Mar 10,2009 10:23:49 AM	emp-dc2.child.xchange.com	-
testhfuser34	testhfuser34	administrator	Mar 10,2009 10:21:57 AM	emp-dc2.child.xchange.com	-
testhfuser23	testhfuser23	Administrator	Mar 10,2009 10:07:03 AM	emp-dc2.child.xchange.com	-
servicedesk	servicedesk	administrator	Mar 07,2009 02:50:26 PM	emp-dc2.child.xchange.com	servicedesk@child.xchange.com
BORB3621	BORB3621	Administrator	Mar 06,2009 02:53:16 PM	emp-dc2.child.xchange.com	-
BORB3621	BORB3621	Administrator	Mar 06,2009 02:53:16 PM	emp-dc2.child.xchange.com	-
BORB3621	BORB3621	Administrator	Mar 06,2009 02:49:43 PM	emp-dc2.child.xchange.com	-
BORB3621	BORB3621	Administrator	Mar 06,2009 02:49:43 PM	emp-dc2.child.xchange.com	-
first1midlast	first1midlast	Administrator	Mar 04,2009 04:16:04 PM	emp-dc2.child.xchange.com	-
first1midlast	first1midlast	Administrator	Mar 04,2009 04:16:04 PM	emp-dc2.child.xchange.com	-
last_mid_first	last_mid_first	Administrator	Mar 04,2009 04:12:57 PM	emp-dc2.child.xchange.com	-
last_mid_first	last_mid_first	Administrator	Mar 04,2009 04:12:57 PM	emp-dc2.child.xchange.com	-
testmbuser42	testmbuser42	administrator	Mar 03,2009 03:02:01 PM	emp-dc2.child.xchange.com	-
testmbuser42	testmbuser42	administrator	Mar 03,2009 03:02:01 PM	emp-dc2.child.xchange.com	-
testmbuser1	testmbuser1	Administrator	Mar 03,2009 02:46:31	emp-dc2.child.xchange.com	

Last Modification on User(s)



Last Modification on Users

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

Select Domain: admp.com

Period: Last 30 Days

Showing : 1-25 of 27 Show 25 per page.

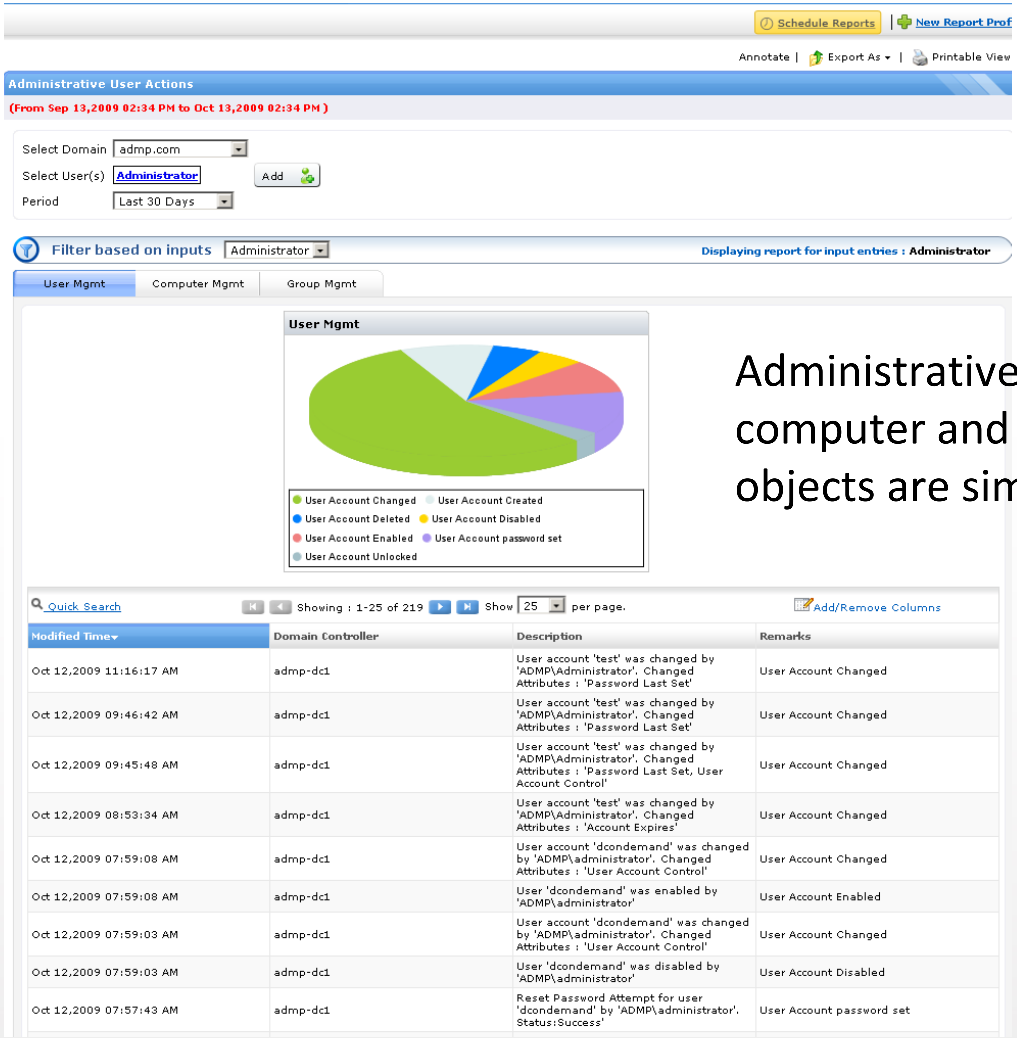
User Name	Caller User Name	Modified Time	Domain Controller	Modified Attributes▾	Remarks
pavunraj	Administrator	Oct 10,2009 10:59:13 AM	admp-dc1	User Workstations	User Account Changed
kala	Administrator	Oct 10,2009 07:38:52 AM	admp-dc1	User Principal Name	User Account Changed
a.z	administrator	Oct 09,2009 01:29:08 PM	admp-dc1	User Parameters	User Account Changed
Allen	Administrator	Oct 10,2009 09:34:24 AM	admp-dc1	User Account Control	User Account Changed
Anandhsamy	Administrator	Oct 09,2009 06:03:21 AM	admp-dc1	User Account Control	User Account Changed
Anandhsamy123	Administrator	Oct 09,2009 08:49:56 AM	admp-dc1	User Account Control	User Account Changed
AnandSamy123	Administrator	Oct 09,2009 08:48:12 AM	admp-dc1	User Account Control	User Account Changed
audituser	Administrator	Oct 09,2009 06:32:04 AM	admp-dc1	User Account Control	User Account Changed
bala	Administrator	Oct 05,2009 02:46:59 PM	admp-dc1	User Account Control	User Account Changed
dcondemand	administrator	Oct 12,2009 07:59:08 AM	admp-dc1	User Account Control	User Account Changed

Last modification done on

Done by

3

Administrative User Action – on user objects



Administrative User Actions

(From Sep 13,2009 02:34 PM to Oct 13,2009 02:34 PM)

Select Domain: admp.com

Select User(s): Administrator

Period: Last 30 Days

Filter based on inputs: Administrator

Displaying report for input entries : **Administrator**

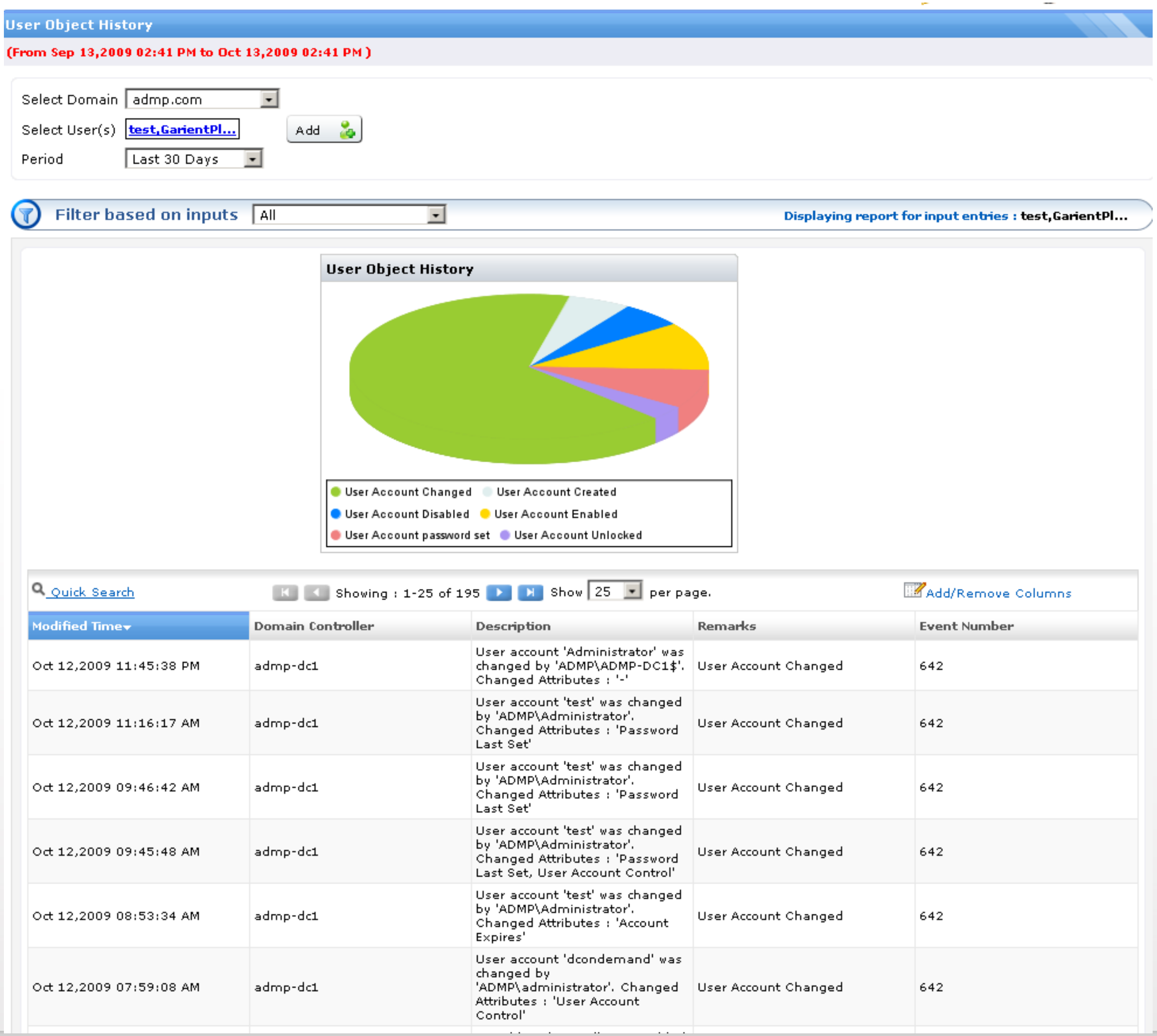
User Mgmt

Showing : 1-25 of 219 Show 25 per page.

Modified Time	Domain Controller	Description	Remarks
Oct 12,2009 11:16:17 AM	admp-dc1	User account 'test' was changed by 'ADMP\Administrator'. Changed Attributes : 'Password Last Set'	User Account Changed
Oct 12,2009 09:46:42 AM	admp-dc1	User account 'test' was changed by 'ADMP\Administrator'. Changed Attributes : 'Password Last Set'	User Account Changed
Oct 12,2009 09:45:48 AM	admp-dc1	User account 'test' was changed by 'ADMP\Administrator'. Changed Attributes : 'Password Last Set, User Account Control'	User Account Changed
Oct 12,2009 08:53:34 AM	admp-dc1	User account 'test' was changed by 'ADMP\Administrator'. Changed Attributes : 'Account Expires'	User Account Changed
Oct 12,2009 07:59:08 AM	admp-dc1	User account 'dcondemand' was changed by 'ADMP\administrator'. Changed Attributes : 'User Account Control'	User Account Changed
Oct 12,2009 07:59:08 AM	admp-dc1	User 'dcondemand' was enabled by 'ADMP\administrator'	User Account Enabled
Oct 12,2009 07:59:03 AM	admp-dc1	User account 'dcondemand' was changed by 'ADMP\administrator'. Changed Attributes : 'User Account Control'	User Account Changed
Oct 12,2009 07:59:03 AM	admp-dc1	User 'dcondemand' was disabled by 'ADMP\administrator'	User Account Disabled
Oct 12,2009 07:57:43 AM	admp-dc1	Reset Password Attempt for user 'dcondemand' by 'ADMP\administrator'. Status:Success'	User Account password set

Administrative user action computer and group objects are similar.

User Object History



User Object History

(From Sep 13,2009 02:41 PM to Oct 13,2009 02:41 PM)

Select Domain: admp.com

Select User(s): test,GarientPl...

Period: Last 30 Days

Filter based on inputs: All

Displaying report for input entries : test,GarientPl...

Showing : 1-25 of 195 Show 25 per page.

Modified Time	Domain Controller	Description	Remarks	Event Number
Oct 12,2009 11:45:38 PM	admp-dc1	User account 'Administrator' was changed by 'ADMP\ADMP-DC1$'. Changed Attributes : '-'	User Account Changed	642
Oct 12,2009 11:16:17 AM	admp-dc1	User account 'test' was changed by 'ADMP\Administrator'. Changed Attributes : 'Password Last Set'	User Account Changed	642
Oct 12,2009 09:46:42 AM	admp-dc1	User account 'test' was changed by 'ADMP\Administrator'. Changed Attributes : 'Password Last Set'	User Account Changed	642
Oct 12,2009 09:45:48 AM	admp-dc1	User account 'test' was changed by 'ADMP\Administrator'. Changed Attributes : 'Password Last Set, User Account Control'	User Account Changed	642
Oct 12,2009 08:53:34 AM	admp-dc1	User account 'test' was changed by 'ADMP\Administrator'. Changed Attributes : 'Account Expires'	User Account Changed	642
Oct 12,2009 07:59:08 AM	admp-dc1	User account 'dcondemand' was changed by 'ADMP\administrator'. Changed Attributes : 'User Account Control'	User Account Changed	642

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

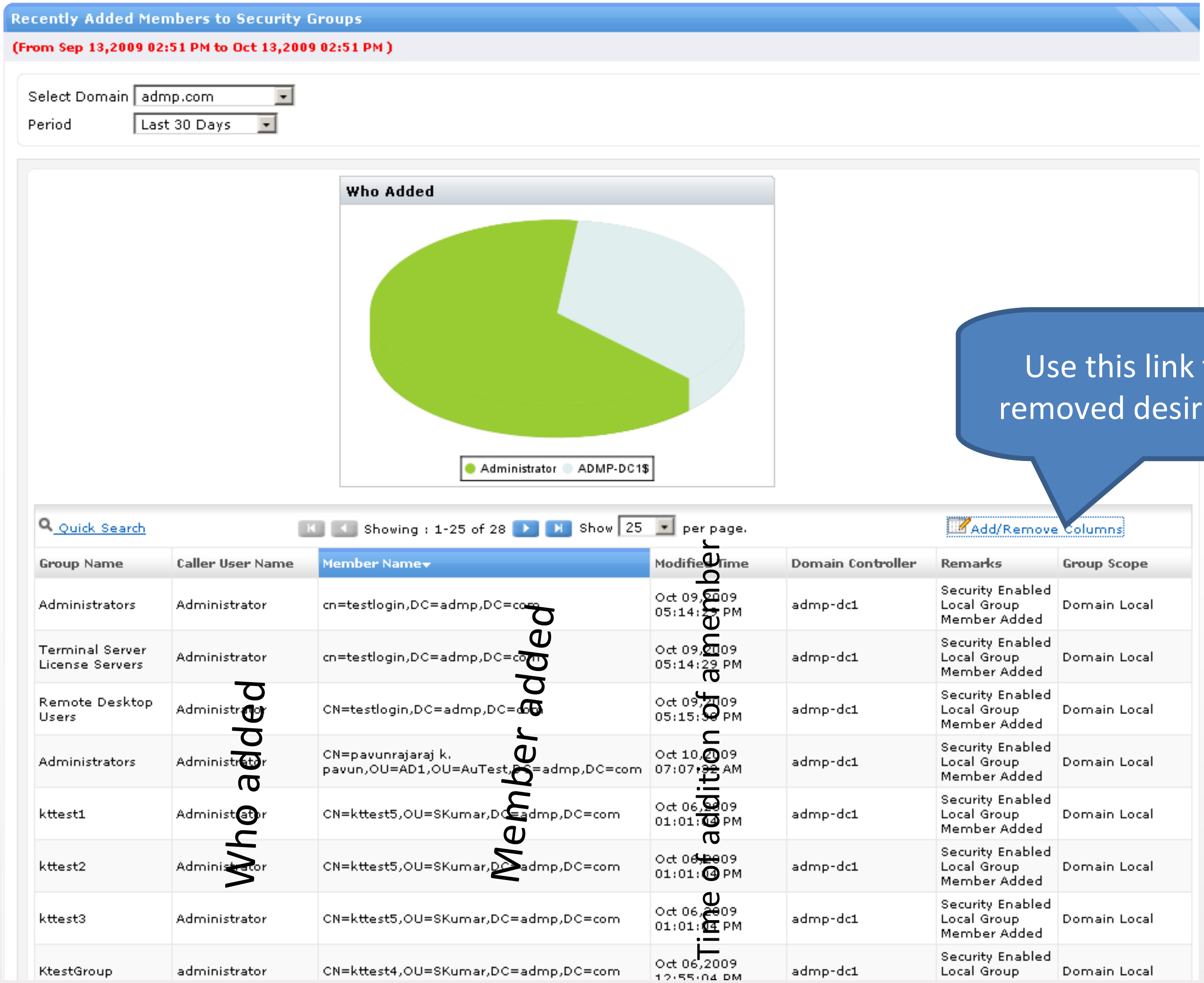
Pre-configured default reports on group management actions and history of changes to groups is listed above.

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



Recently Added Members to Security Groups

(From Sep 13,2009 02:51 PM to Oct 13,2009 02:51 PM)

Select Domain: admp.com

Period: Last 30 Days

Who Added

● Administrator ● ADMP-DC1$

Quick Search | Showing : 1-25 of 28 | Show 25 per page. | Add/Remove Columns

Group Name	Caller User Name	Member Name	Modified Time	Domain Controller	Remarks	Group Scope
Administrators	Administrator	cn=testlogin,DC=admp,DC=com	Oct 09,2009 05:14:2[illegible] PM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
Terminal Server License Servers	Administrator	cn=testlogin,DC=admp,DC=com	Oct 09,2009 05:14:29 PM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
Remote Desktop Users	Administrator	CN=testlogin,DC=admp,DC=com	Oct 09,2009 05:15:3[illegible] PM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
Administrators	Administrator	CN=pavunrajaraj k. pavun,OU=AD1,OU=AuTest,DC=admp,DC=com	Oct 10,2009 07:07:3[illegible] AM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
kttest1	Administrator	CN=kttest5,OU=SKumar,DC=admp,DC=com	Oct 06,2009 01:01:04 PM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
kttest2	Administrator	CN=kttest5,OU=SKumar,DC=admp,DC=com	Oct 06,2009 01:01:04 PM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
kttest3	Administrator	CN=kttest5,OU=SKumar,DC=admp,DC=com	Oct 06,2009 01:01:04 PM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
KtestGroup	administrator	CN=kttest4,OU=SKumar,DC=admp,DC=com	Oct 06,2009 12:55:04 PM	admp-dc1	Security Enabled Local Group	Domain Local

Who added

Member added

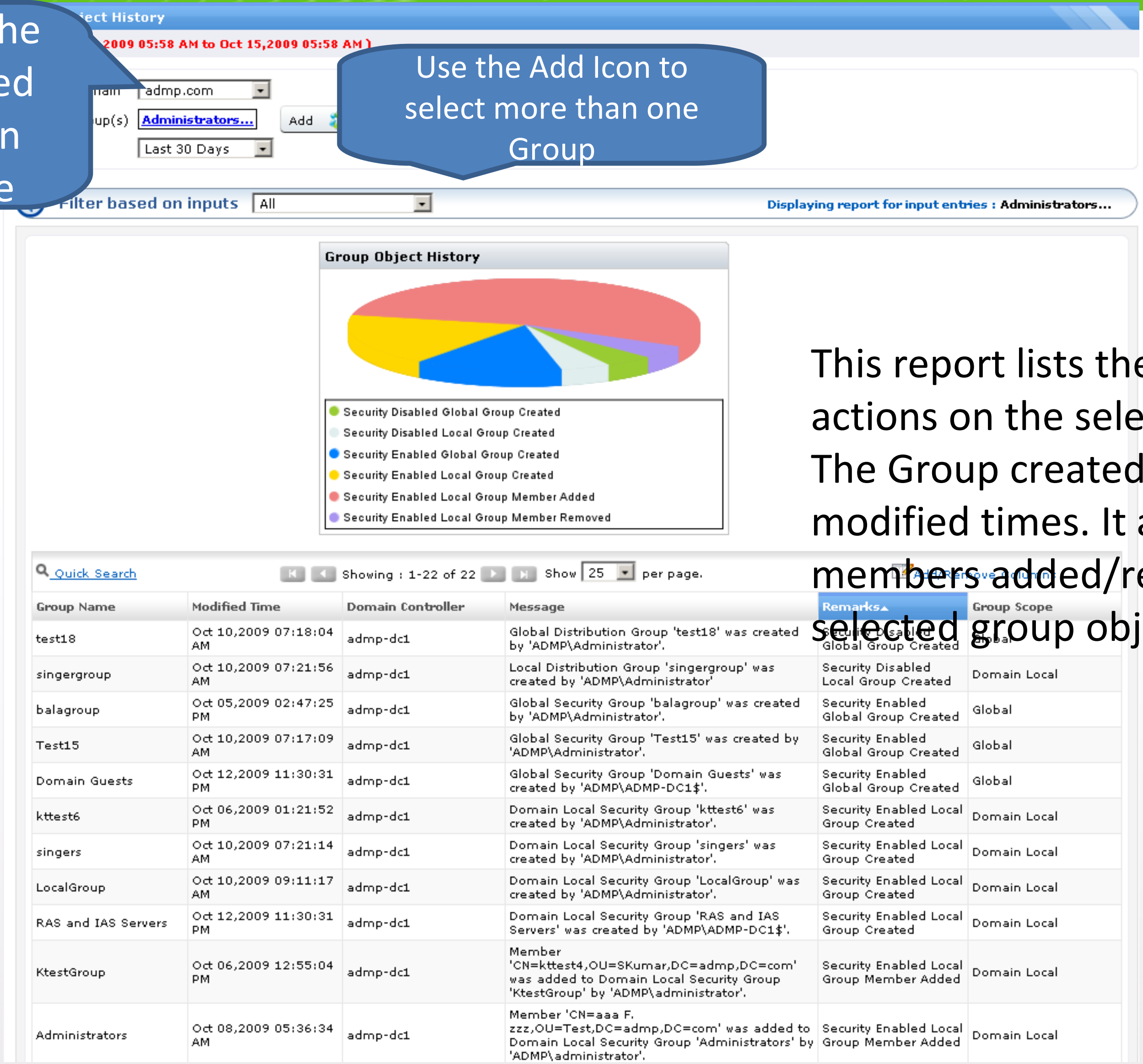
Time of addition of amember

Use this link to add or removed desired columns

Group Object History

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

Use the Add Icon to select more than one Group



ject History

2009 05:58 AM to Oct 15,2009 05:58 AM)

main: admp.com

up(s): Administrators... Add

Last 30 Days

Filter based on inputs: All

Displaying report for input entries : Administrators...

Group Object History

● Security Disabled Global Group Created
● Security Disabled Local Group Created
● Security Enabled Global Group Created
● Security Enabled Local Group Created
● Security Enabled Local Group Member Added
● Security Enabled Local Group Member Removed
Quick Search
Add/Remove Columns

Showing : 1-22 of 22 Show 25 per page.

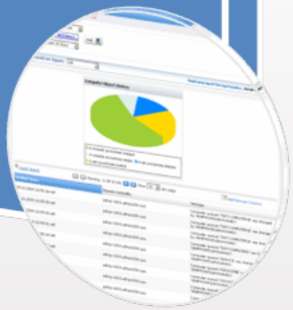
Group Name	Modified Time	Domain Controller	Message	Remarks▴	Group Scope
test18	Oct 10,2009 07:18:04 AM	admp-dc1	Global Distribution Group 'test18' was created by 'ADMP\Administrator'.	Security Disabled Global Group Created	Global
singergroup	Oct 10,2009 07:21:56 AM	admp-dc1	Local Distribution Group 'singergroup' was created by 'ADMP\Administrator'	Security Disabled Local Group Created	Domain Local
balagroup	Oct 05,2009 02:47:25 PM	admp-dc1	Global Security Group 'balagroup' was created by 'ADMP\Administrator'.	Security Enabled Global Group Created	Global
Test15	Oct 10,2009 07:17:09 AM	admp-dc1	Global Security Group 'Test15' was created by 'ADMP\Administrator'.	Security Enabled Global Group Created	Global
Domain Guests	Oct 12,2009 11:30:31 PM	admp-dc1	Global Security Group 'Domain Guests' was created by 'ADMP\ADMP-DC1$'.	Security Enabled Global Group Created	Global
kttest6	Oct 06,2009 01:21:52 PM	admp-dc1	Domain Local Security Group 'kttest6' was created by 'ADMP\Administrator'.	Security Enabled Local Group Created	Domain Local
singers	Oct 10,2009 07:21:14 AM	admp-dc1	Domain Local Security Group 'singers' was created by 'ADMP\Administrator'.	Security Enabled Local Group Created	Domain Local
LocalGroup	Oct 10,2009 09:11:17 AM	admp-dc1	Domain Local Security Group 'LocalGroup' was created by 'ADMP\Administrator'.	Security Enabled Local Group Created	Domain Local
RAS and IAS Servers	Oct 12,2009 11:30:31 PM	admp-dc1	Domain Local Security Group 'RAS and IAS Servers' was created by 'ADMP\ADMP-DC1$'.	Security Enabled Local Group Created	Domain Local
KtestGroup	Oct 06,2009 12:55:04 PM	admp-dc1	Member 'CN=kttest4,OU=SKumar,DC=admp,DC=com' was added to Domain Local Security Group 'KtestGroup' by 'ADMP\administrator'.	Security Enabled Local Group Member Added	Domain Local
Administrators	Oct 08,2009 05:36:34 AM	admp-dc1	Member 'CN=aaa F. zzz,OU=Test,DC=admp,DC=com' was added to Domain Local Security Group 'Administrators' by 'ADMP\administrator'.	Security Enabled Local Group Member Added	Domain Local

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).

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.

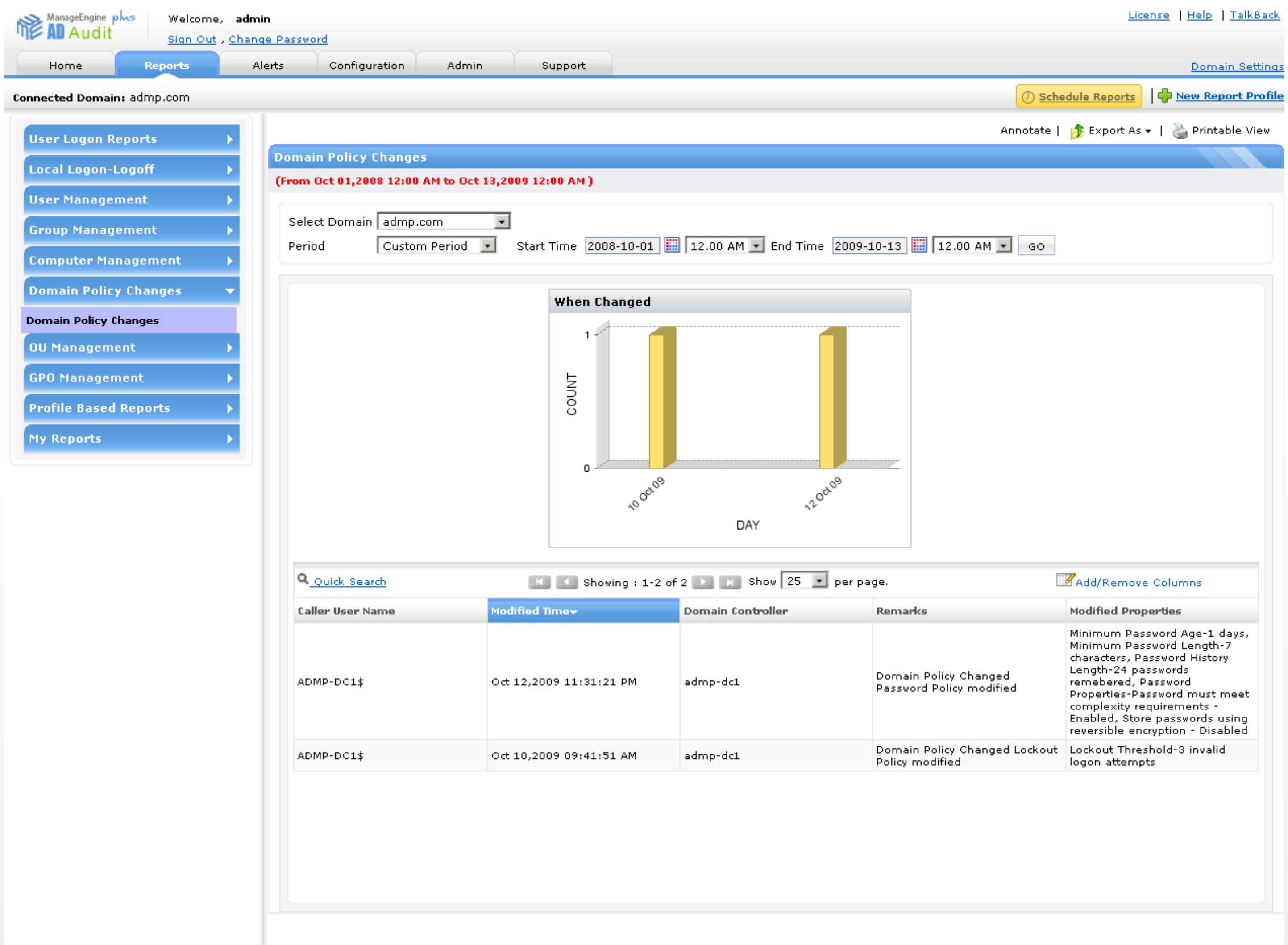


Domain Policy Changes

- Domain policy change report.

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

Domain Policy change information



Connected Domain: admp.com

Domain Policy Changes

(From Oct 01,2008 12:00 AM to Oct 13,2009 12:00 AM)

Select Domain: admp.com

Period: Custom Period   Start Time: 2008-10-01 12.00 AM   End Time: 2009-10-13 12.00 AM   GO

Showing : 1-2 of 2   Show 25 per page.

Caller User Name	Modified Time	Domain Controller	Remarks	Modified Properties
ADMP-DC1$	Oct 12,2009 11:31:21 PM	admp-dc1	Domain Policy Changed Password Policy modified	Minimum Password Age-1 days, Minimum Password Length-7 characters, Password History Length-24 passwords remembered, Password Properties-Password must meet complexity requirements - Enabled, Store passwords using reversible encryption - Disabled
ADMP-DC1$	Oct 10,2009 09:41:51 AM	admp-dc1	Domain Policy Changed Lockout Policy modified	Lockout Threshold-3 invalid logon attempts

OU Management Reports

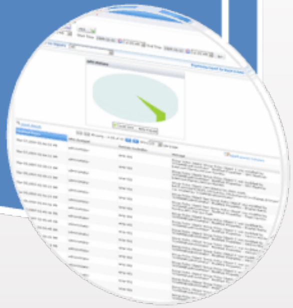
- Recently Created OUs
- Recently Deleted OUs
- Recently Modified OUs
- OU History

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

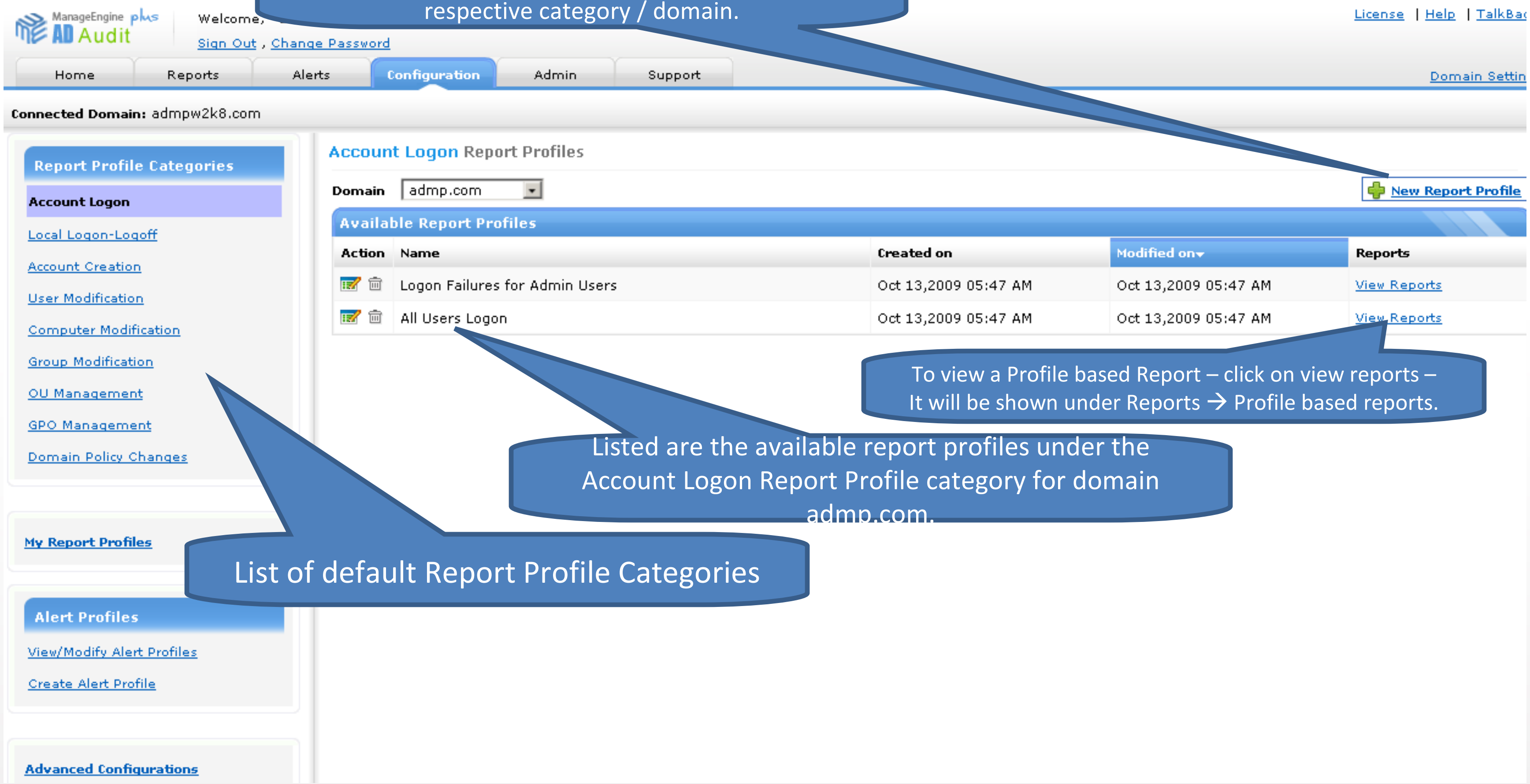
Pre-configured default audit reports provided by ADAudit Plus for GPO Management changes are listed above.



Profile Based Reports

- A profile based report is defined(created)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 view 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



Welcome,

Sign Out , Change Password

License | Help | TalkBa

Connected Domain: admpw2k8.com

Report Profile Categories

- **Account Logon**
- Local Logon-Logoff
- Account Creation
- User Modification
- Computer Modification
- Group Modification
- OU Management
- GPO Management
- Domain Policy Changes

My Report Profiles

Alert Profiles

- View/Modify Alert Profiles
- Create Alert Profile

Advanced Configurations

Account Logon Report Profiles

Domain admp.com

New Report Profile

Available Report Profiles

Action	Name	Created on	Modified on	Reports
	Logon Failures for Admin Users	Oct 13,2009 05:47 AM	Oct 13,2009 05:47 AM	View Reports
	All Users Logon	Oct 13,2009 05:47 AM	Oct 13,2009 05:47 AM	View Reports

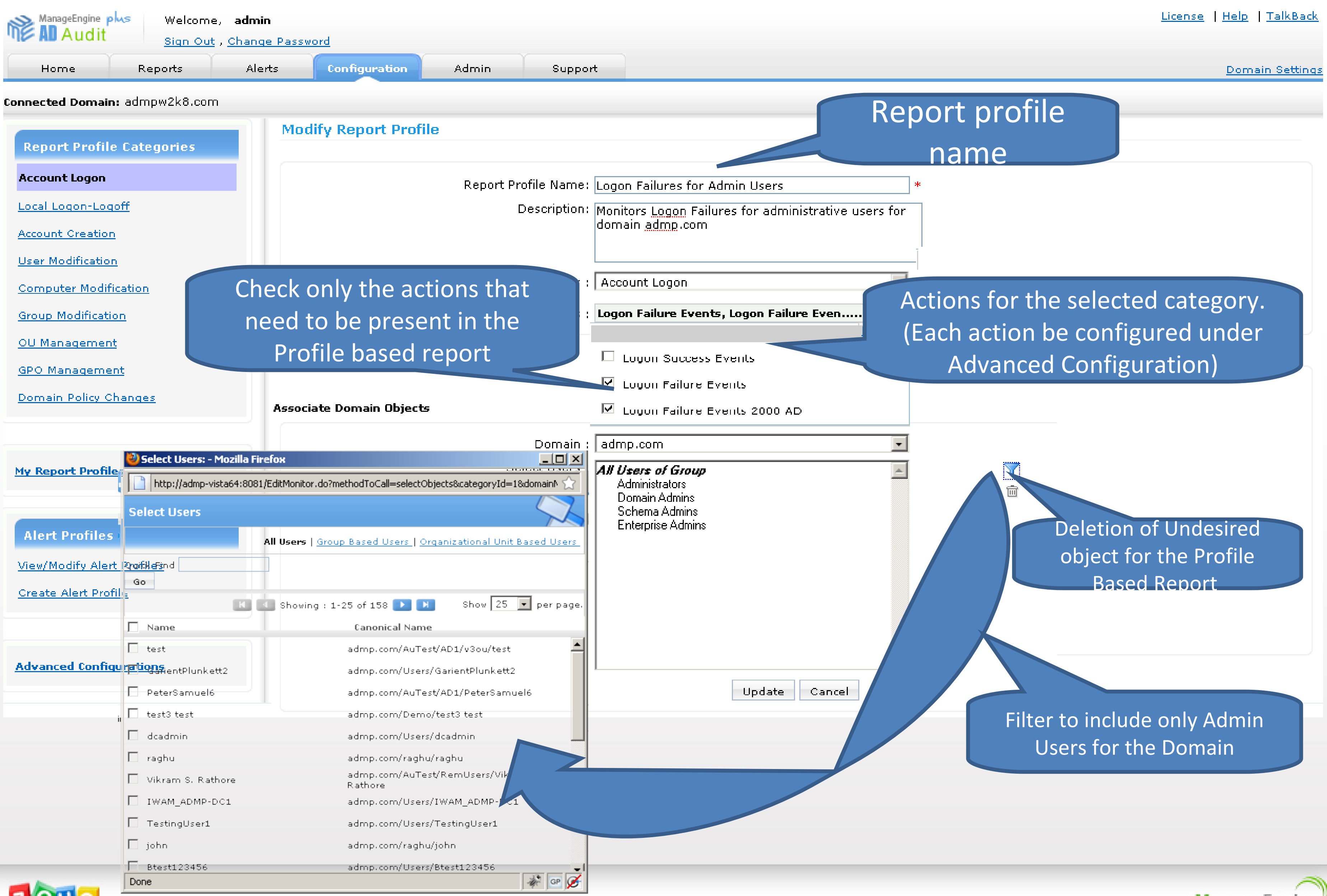
To configure your own report profile click here. The report profiles created will be listed under their respective category / domain.

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

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

List of default Report Profile Categories

Configuring a report profile -2



ManageEngine AD Audit plus

Welcome, **admin**

Sign Out , Change Password

License | Help | TalkBack

Home | Reports | Alerts | Configuration | Admin | Support

Domain Settings

Connected Domain: admpw2k8.com

Report Profile Categories

Account Logon

Local Logon-Logoff

Account Creation

User Modification

Computer Modification

Group Modification

OU Management

GPO Management

Domain Policy Changes

My Report Profiles

Alert Profiles

View/Modify Alert Profiles

Create Alert Profile

Advanced Configurations

Modify Report Profile

Report Profile Name: Logon Failures for Admin Users *

Description: Monitors Logon Failures for administrative users for domain admp.com

: Account Logon

: Logon Failure Events, Logon Failure Even.....

□ Logon Success Events

☑ Logon Failure Events

☑ Logon Failure Events 2000 AD

Associate Domain Objects

Domain : admp.com

All Users of Group
Administrators
Domain Admins
Schema Admins
Enterprise Admins

Update | Cancel

Select Users: - Mozilla Firefox

http://admp-vista64:8081/EditMonitor.do?methodToCall=selectObjects&categoryId=1&domainN

Select Users

All Users | Group Based Users | Organizational Unit Based Users

Find | Go

Showing : 1-25 of 158 | Show 25 per page.

□ Name	Canonical Name
□ test	admp.com/AuTest/AD1/v3ou/test
□ GarientPlunkett2	admp.com/Users/GarientPlunkett2
□ PeterSamuel6	admp.com/AuTest/AD1/PeterSamuel6
□ test3 test	admp.com/Demo/test3 test
□ dcadmin	admp.com/Users/dcadmin
□ raghu	admp.com/raghu/raghu
□ Vikram S. Rathore	admp.com/AuTest/RemUsers/Vik Rathore
□ IWAM_ADMP-DC1	admp.com/Users/IWAM_ADMP-DC1
□ TestingUser1	admp.com/Users/TestingUser1
□ john	admp.com/raghu/john
□ Btest123456	admp.com/Users/Btest123456

Done

Report profile name

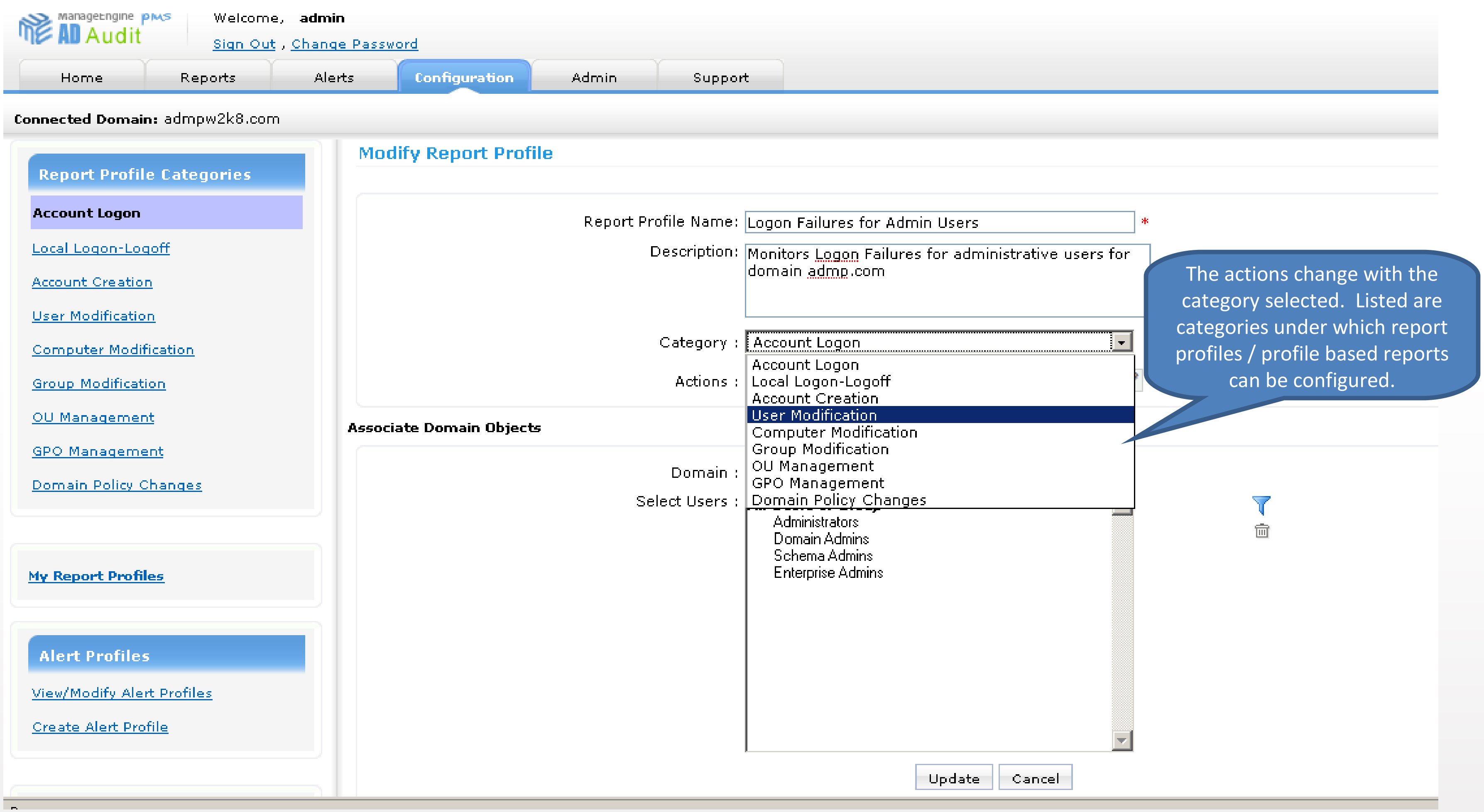
Check only the actions that need to be present in the Profile based report

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

Configuration of a report profile - 3



Connected Domain: admpw2k8.com

Modify Report Profile

Report Profile Name: Logon Failures for Admin Users *

Description: Monitors Logon Failures for administrative users for domain admp.com

Category : Account Logon

Actions :

- Account Logon
- Local Logon-Logoff
- Account Creation
- User Modification
- Computer Modification
- Group Modification
- OU Management
- GPO Management
- Domain Policy Changes

Associate Domain Objects

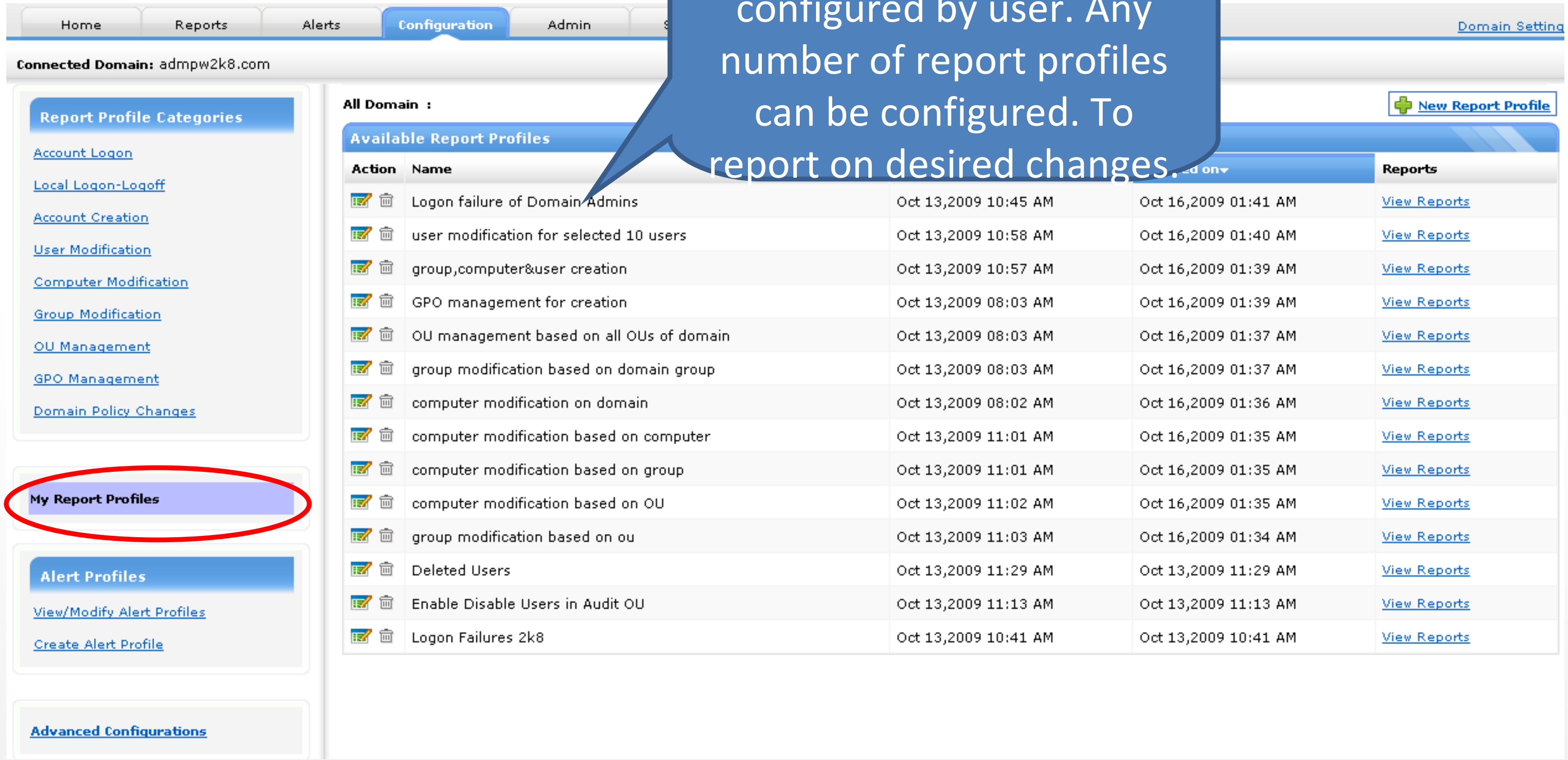
Domain :

Select Users :

- Administrators
- Domain Admins
- Schema Admins
- Enterprise Admins

The actions change with the category selected. Listed are categories under which report profiles / profile based reports can be configured.

My Report Profiles



Connected Domain: admpw2k8.com

Report Profile Categories

- Account Logon
- Local Logon-Logoff
- Account Creation
- User Modification
- Computer Modification
- Group Modification
- OU Management
- GPO Management
- Domain Policy Changes

My Report Profiles

Alert Profiles

- View/Modify Alert Profiles
- Create Alert Profile

Advanced Configurations

All Domain :

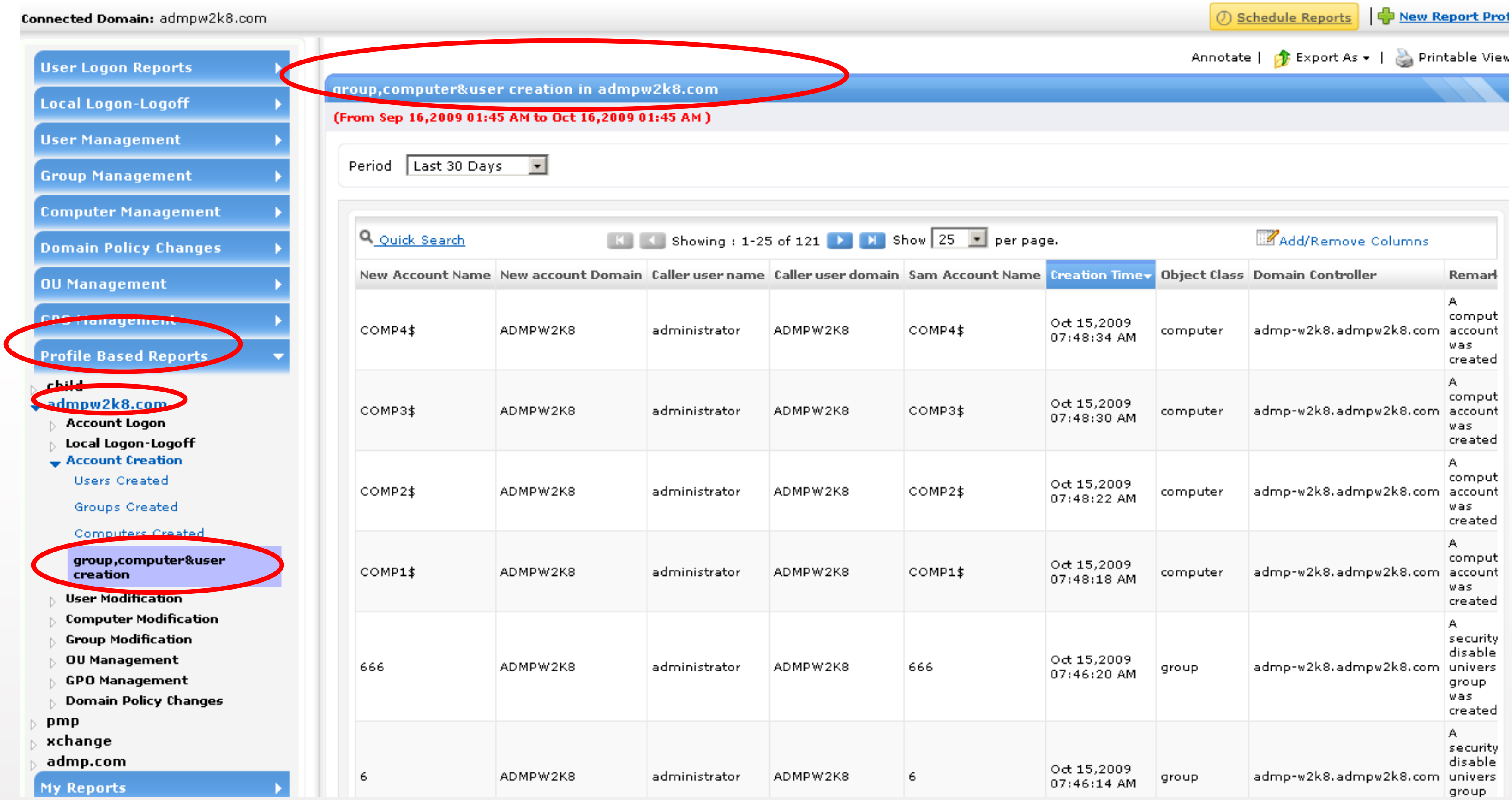
New Report Profile

Available Report Profiles

Action	Name		d on▾	Reports
	Logon failure of Domain Admins	Oct 13,2009 10:45 AM	Oct 16,2009 01:41 AM	View Reports
	user modification for selected 10 users	Oct 13,2009 10:58 AM	Oct 16,2009 01:40 AM	View Reports
	group,computer&user creation	Oct 13,2009 10:57 AM	Oct 16,2009 01:39 AM	View Reports
	GPO management for creation	Oct 13,2009 08:03 AM	Oct 16,2009 01:39 AM	View Reports
	OU management based on all OUs of domain	Oct 13,2009 08:03 AM	Oct 16,2009 01:37 AM	View Reports
	group modification based on domain group	Oct 13,2009 08:03 AM	Oct 16,2009 01:37 AM	View Reports
	computer modification on domain	Oct 13,2009 08:02 AM	Oct 16,2009 01:36 AM	View Reports
	computer modification based on computer	Oct 13,2009 11:01 AM	Oct 16,2009 01:35 AM	View Reports
	computer modification based on group	Oct 13,2009 11:01 AM	Oct 16,2009 01:35 AM	View Reports
	computer modification based on OU	Oct 13,2009 11:02 AM	Oct 16,2009 01:35 AM	View Reports
	group modification based on ou	Oct 13,2009 11:03 AM	Oct 16,2009 01:34 AM	View Reports
	Deleted Users	Oct 13,2009 11:29 AM	Oct 13,2009 11:29 AM	View Reports
	Enable Disable Users in Audit OU	Oct 13,2009 11:13 AM	Oct 13,2009 11:13 AM	View Reports
	Logon Failures 2k8	Oct 13,2009 10:41 AM	Oct 13,2009 10:41 AM	View Reports

List of Report Profiles configured by user. Any number of report profiles can be configured. To report on desired changes.

Profile Based Report



Connected Domain: admpw2k8.com

group,computer&user creation in admpw2k8.com

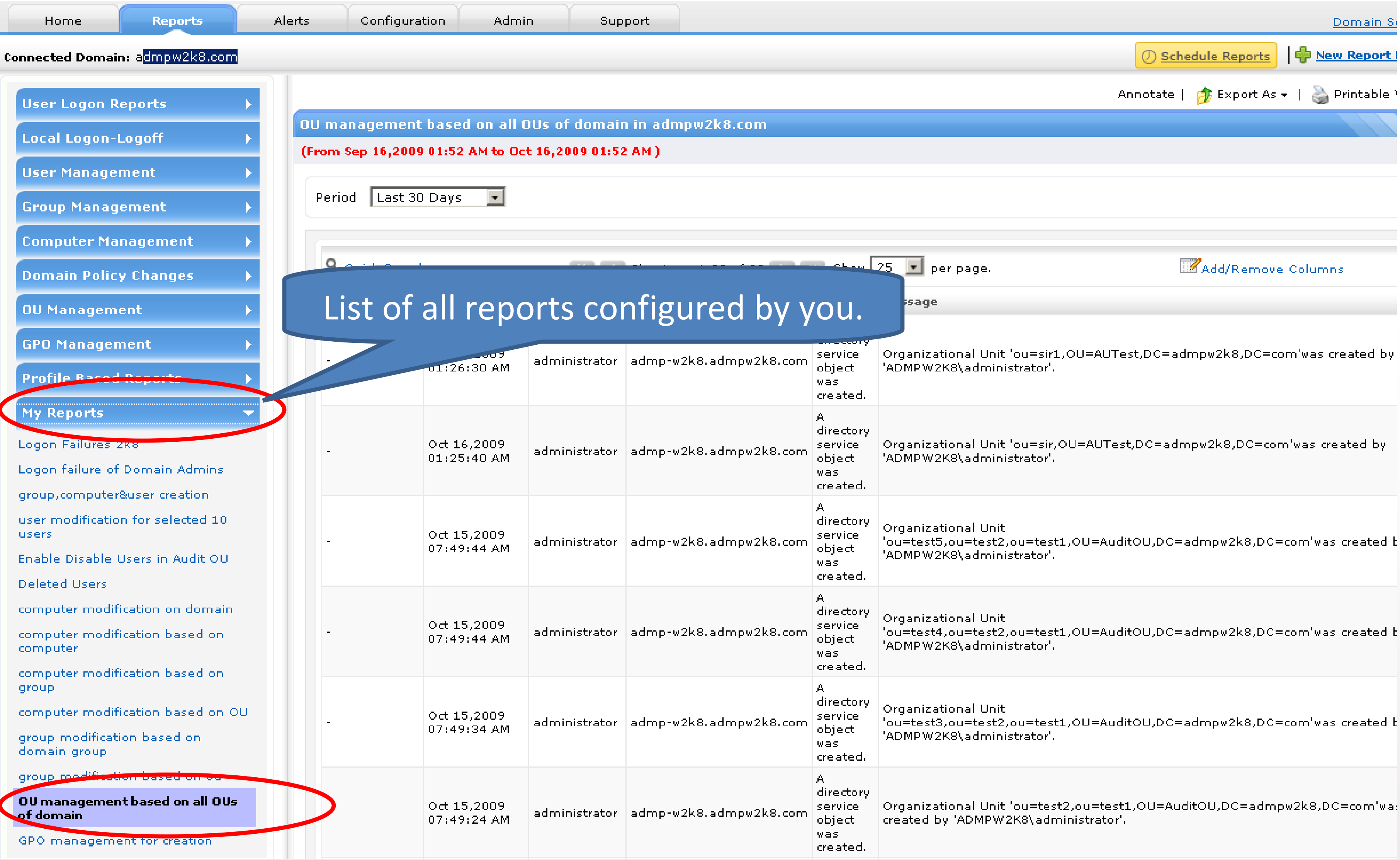
(From Sep 16,2009 01:45 AM to Oct 16,2009 01:45 AM)

Period: Last 30 Days

Showing : 1-25 of 121 Show 25 per page.

New Account Name	New account Domain	Caller user name	Caller user domain	Sam Account Name	Creation Time	Object Class	Domain Controller	Remark
COMP4$	ADMPW2K8	administrator	ADMPW2K8	COMP4$	Oct 15,2009 07:48:34 AM	computer	admp-w2k8.admpw2k8.com	A comput account was created
COMP3$	ADMPW2K8	administrator	ADMPW2K8	COMP3$	Oct 15,2009 07:48:30 AM	computer	admp-w2k8.admpw2k8.com	A comput account was created
COMP2$	ADMPW2K8	administrator	ADMPW2K8	COMP2$	Oct 15,2009 07:48:22 AM	computer	admp-w2k8.admpw2k8.com	A comput account was created
COMP1$	ADMPW2K8	administrator	ADMPW2K8	COMP1$	Oct 15,2009 07:48:18 AM	computer	admp-w2k8.admpw2k8.com	A comput account was created
666	ADMPW2K8	administrator	ADMPW2K8	666	Oct 15,2009 07:46:20 AM	group	admp-w2k8.admpw2k8.com	A security disable univers group was created
6	ADMPW2K8	administrator	ADMPW2K8	6	Oct 15,2009 07:46:14 AM	group	admp-w2k8.admpw2k8.com	A security disable univers group

My Reports



Home | Reports | Alerts | Configuration | Admin | Support

Domain S

Connected Domain: admpw2k8.com

Schedule Reports | New Report

Annotate | Export As | Printable

- User Logon Reports
- Local Logon-Logoff
- User Management
- Group Management
- Computer Management
- Domain Policy Changes
- OU Management
- GPO Management
- Profile Based Reports
- My Reports
  - Logon Failures 2k8
  - Logon failure of Domain Admins
  - group,computer&user creation
  - user modification for selected 10 users
  - Enable Disable Users in Audit OU
  - Deleted Users
  - computer modification on domain
  - computer modification based on computer
  - computer modification based on group
  - computer modification based on OU
  - group modification based on domain group
  - group modification based on ou
  - **OU management based on all OUs of domain**
  - GPO management for creation

OU management based on all OUs of domain in admpw2k8.com

(From Sep 16,2009 01:52 AM to Oct 16,2009 01:52 AM)

Period: Last 30 Days

Show 25 per page.

Add/Remove Columns

					ssage
-	01:26:30 AM	administrator	admp-w2k8.admpw2k8.com	service object was created.	Organizational Unit 'ou=sir1,OU=AUTest,DC=admpw2k8,DC=com'was created by 'ADMPW2K8\administrator'.
-	Oct 16,2009 01:25:40 AM	administrator	admp-w2k8.admpw2k8.com	A directory service object was created.	Organizational Unit 'ou=sir,OU=AUTest,DC=admpw2k8,DC=com'was created by 'ADMPW2K8\administrator'.
-	Oct 15,2009 07:49:44 AM	administrator	admp-w2k8.admpw2k8.com	A directory service object was created.	Organizational Unit 'ou=test5,ou=test2,ou=test1,OU=AuditOU,DC=admpw2k8,DC=com'was created b 'ADMPW2K8\administrator'.
-	Oct 15,2009 07:49:44 AM	administrator	admp-w2k8.admpw2k8.com	A directory service object was created.	Organizational Unit 'ou=test4,ou=test2,ou=test1,OU=AuditOU,DC=admpw2k8,DC=com'was created b 'ADMPW2K8\administrator'.
-	Oct 15,2009 07:49:34 AM	administrator	admp-w2k8.admpw2k8.com	A directory service object was created.	Organizational Unit 'ou=test3,ou=test2,ou=test1,OU=AuditOU,DC=admpw2k8,DC=com'was created b 'ADMPW2K8\administrator'.
-	Oct 15,2009 07:49:24 AM	administrator	admp-w2k8.admpw2k8.com	A directory service object was created.	Organizational Unit 'ou=test2,ou=test1,OU=AuditOU,DC=admpw2k8,DC=com'wa: created by 'ADMPW2K8\administrator'.

List of all reports configured by you.

Alerts Tab of ADAudit Plus

Also explained configuration of Alerts

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

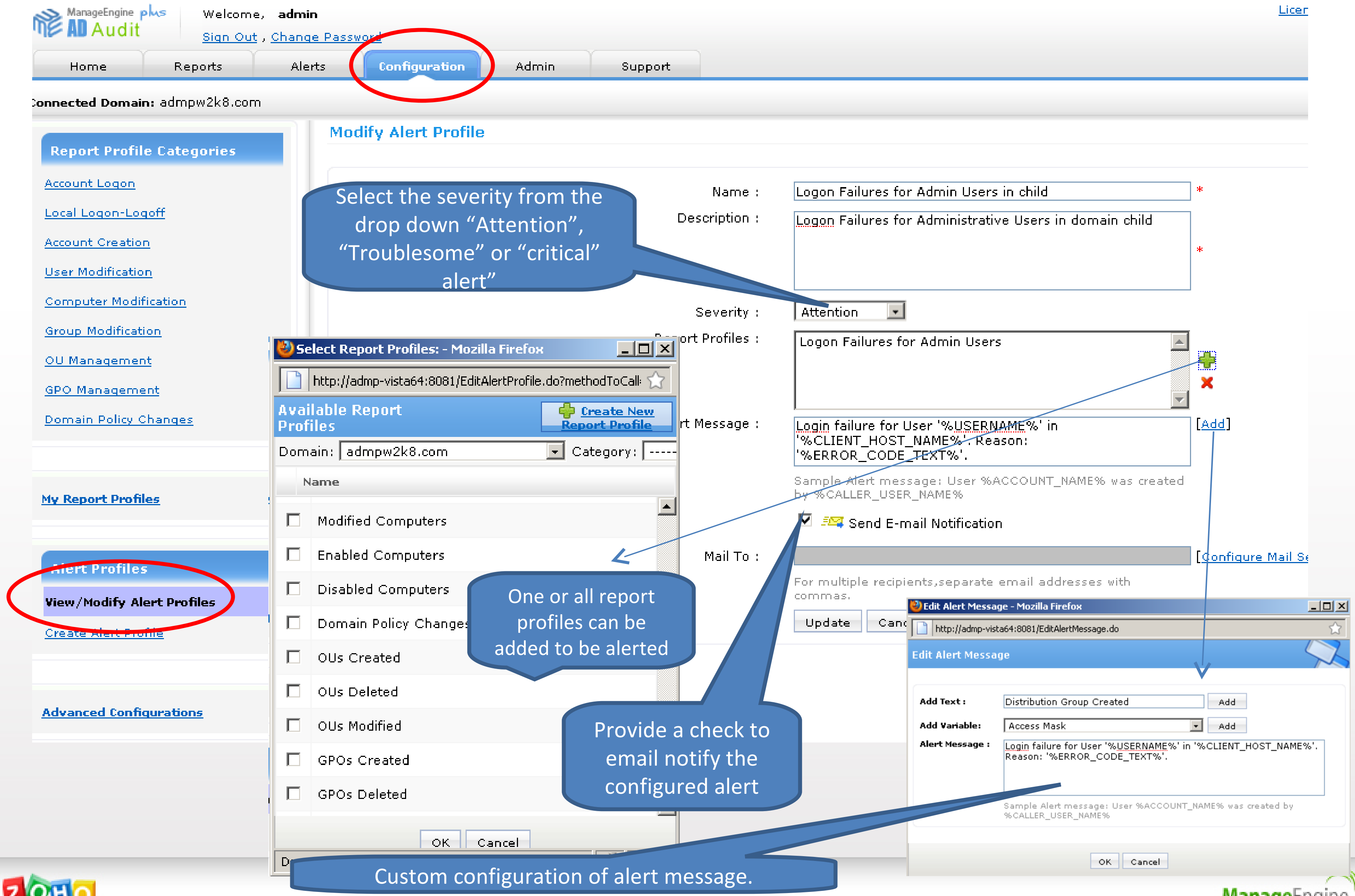
Alert Profile Based Alerts and

Report Profile Based Alerts

Alert Profile Based Alert

- 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



Connected Domain: admpw2k8.com

Modify Alert Profile

Name :	Logon Failures for Admin Users in child *
Description :	Logon Failures for Administrative Users in domain child *
Severity :	Attention
Report Profiles :	Logon Failures for Admin Users
Alert Message :	Login failure for User '%USERNAME%' in '%CLIENT_HOST_NAME%'. Reason: '%ERROR_CODE_TEXT%'. [Add]

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

☑ Send E-mail Notification

Mail To : [Configure Mail Se

For multiple recipients,separate email addresses with commas.

Select Report Profiles: - Mozilla Firefox

http://admp-vista64:8081/EditAlertProfile.do?methodToCall

Available Report Profiles — Create New Report Profile

Domain: admpw2k8.com Category: -----

	Name
□	Modified Computers
□	Enabled Computers
□	Disabled Computers
□	Domain Policy Changes
□	OUs Created
□	OUs Deleted
□	OUs Modified
□	GPOs Created
□	GPOs Deleted

Edit Alert Message - Mozilla Firefox

http://admp-vista64:8081/EditAlertMessage.do

Edit Alert Message

Add Text :	Distribution Group Created [Add]
Add Variable:	Access Mask [Add]
Alert Message :	Login failure for User '%USERNAME%' in '%CLIENT_HOST_NAME%'. Reason: '%ERROR_CODE_TEXT%'.

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

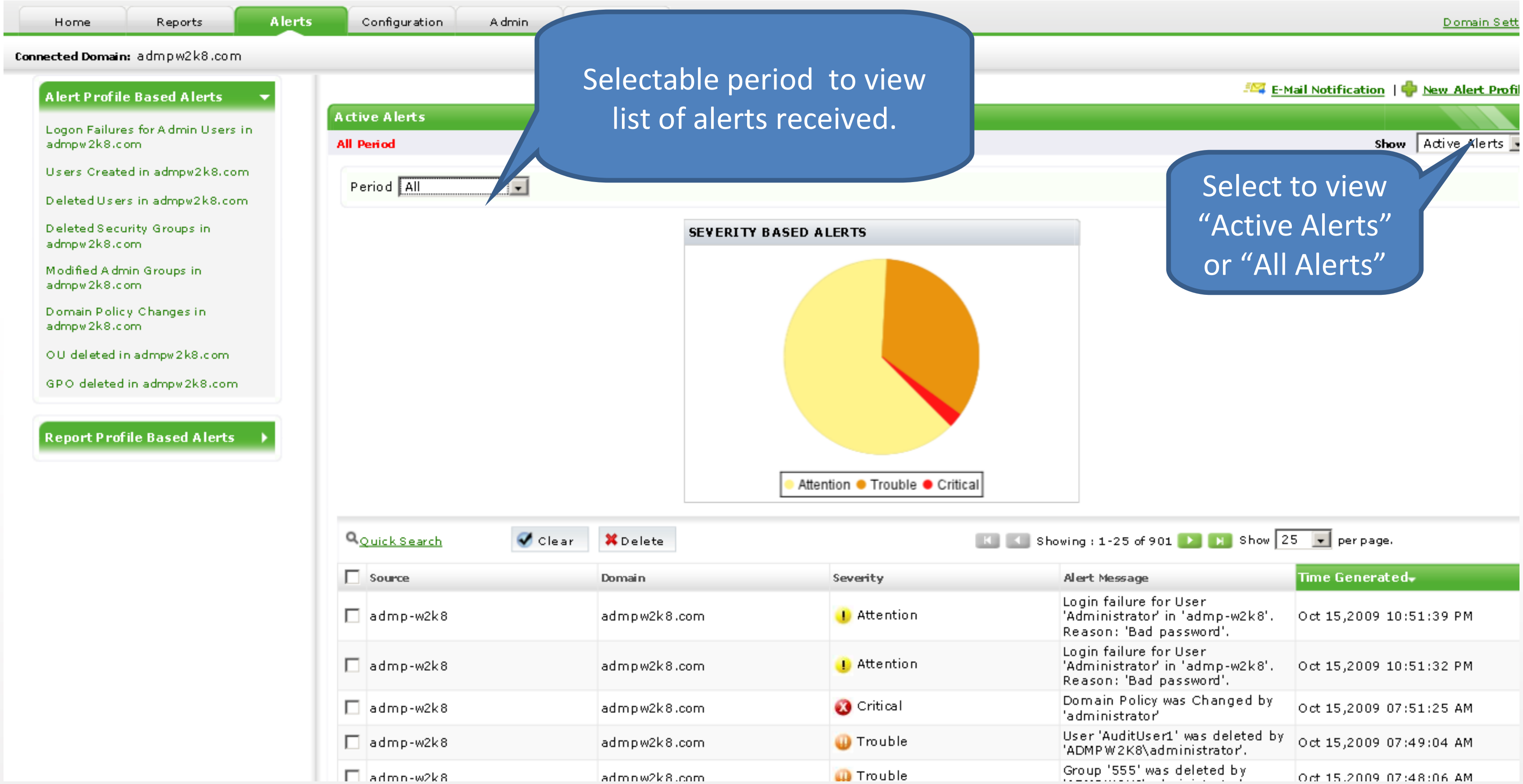
Select the severity from the drop down “Attention”, “Troublesome” or “critical” alert”

One or all report profiles can be added to be alerted

Provide a check to email notify the configured alert

Custom configuration of alert message.

Active Alert seen from the product



Connected Domain: admpw2k8.com

Alert Profile Based Alerts

- Logon Failures for Admin Users in admpw2k8.com
- Users Created in admpw2k8.com
- Deleted Users in admpw2k8.com
- Deleted Security Groups in admpw2k8.com
- Modified Admin Groups in admpw2k8.com
- Domain Policy Changes in admpw2k8.com
- OU deleted in admpw2k8.com
- GPO deleted in admpw2k8.com

Report Profile Based Alerts

Active Alerts

All Period

Show: Active Alerts

Period: All

SEVERITY BASED ALERTS

Showing : 1-25 of 901 Show 25 per page.

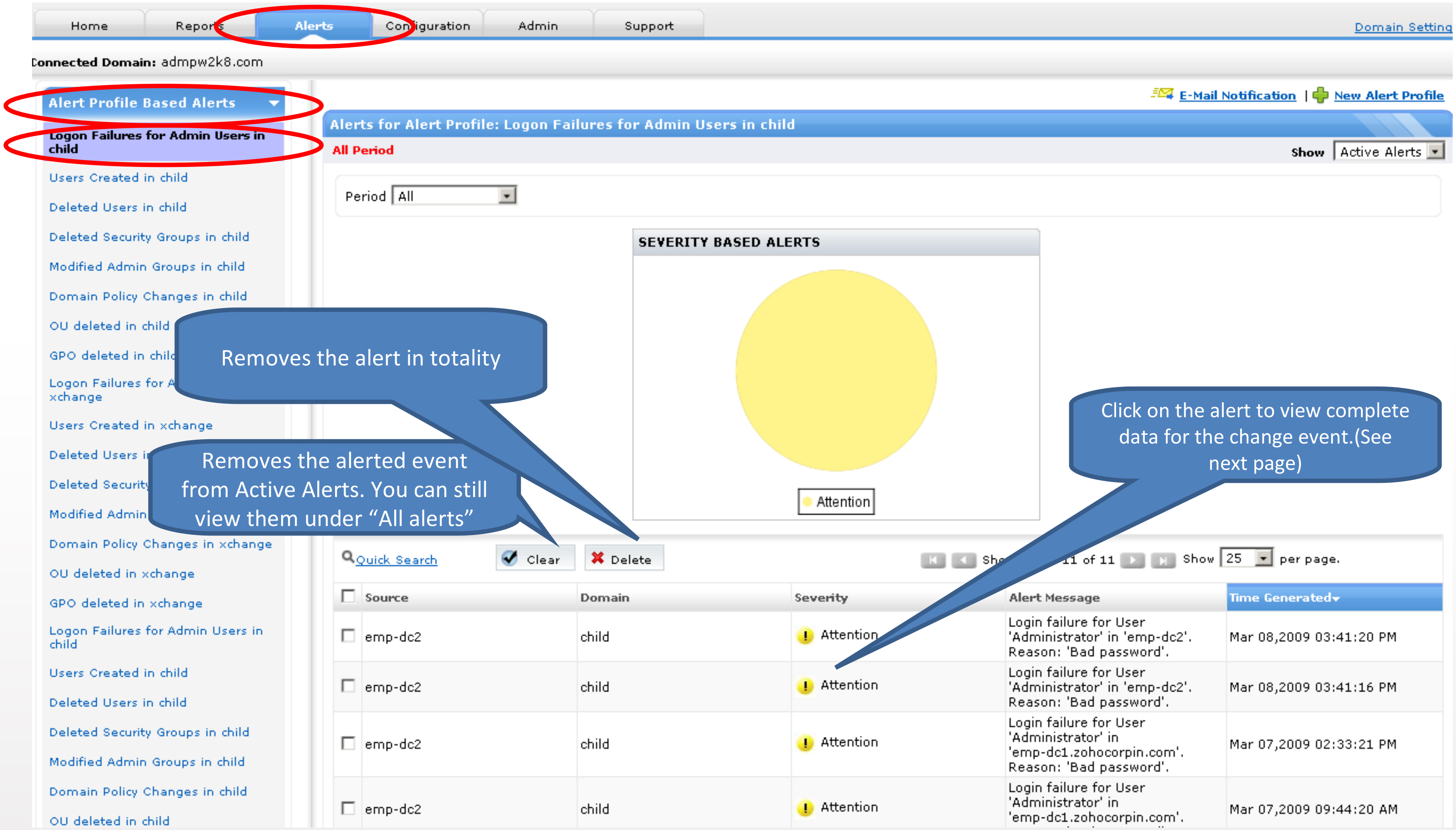
□	Source	Domain	Severity	Alert Message	Time Generated
□	admp-w2k8	admpw2k8.com	Attention	Login failure for User 'Administrator' in 'admp-w2k8'. Reason: 'Bad password'.	Oct 15,2009 10:51:39 PM
□	admp-w2k8	admpw2k8.com	Attention	Login failure for User 'Administrator' in 'admp-w2k8'. Reason: 'Bad password'.	Oct 15,2009 10:51:32 PM
□	admp-w2k8	admpw2k8.com	Critical	Domain Policy was Changed by 'administrator'	Oct 15,2009 07:51:25 AM
□	admp-w2k8	admpw2k8.com	Trouble	User 'AuditUser1' was deleted by 'ADMPW2K8\administrator'.	Oct 15,2009 07:49:04 AM
□	admp-w2k8	admpw2k8.com	Trouble	Group '555' was deleted by	Oct 15,2009 07:48:06 AM

Selectable period to view list of alerts received.

Select to view "Active Alerts" or "All Alerts"

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

Viewing a Alert Profile Based Alert



Connected Domain: admpw2k8.com

Logon Failures for Admin Users in child

Users Created in child
Deleted Users in child
Deleted Security Groups in child
Modified Admin Groups in child
Domain Policy Changes in child
OU deleted in child
GPO deleted in child
Logon Failures for A… xchange
Users Created in xchange
Deleted Users i…
Deleted Security…
Modified Admin…
Domain Policy Changes in xchange
OU deleted in xchange
GPO deleted in xchange
Logon Failures for Admin Users in child
Users Created in child
Deleted Users in child
Deleted Security Groups in child
Modified Admin Groups in child
Domain Policy Changes in child
OU deleted in child

Alerts for Alert Profile: Logon Failures for Admin Users in child

All Period

Show: Active Alerts

Period: All

SEVERITY BASED ALERTS

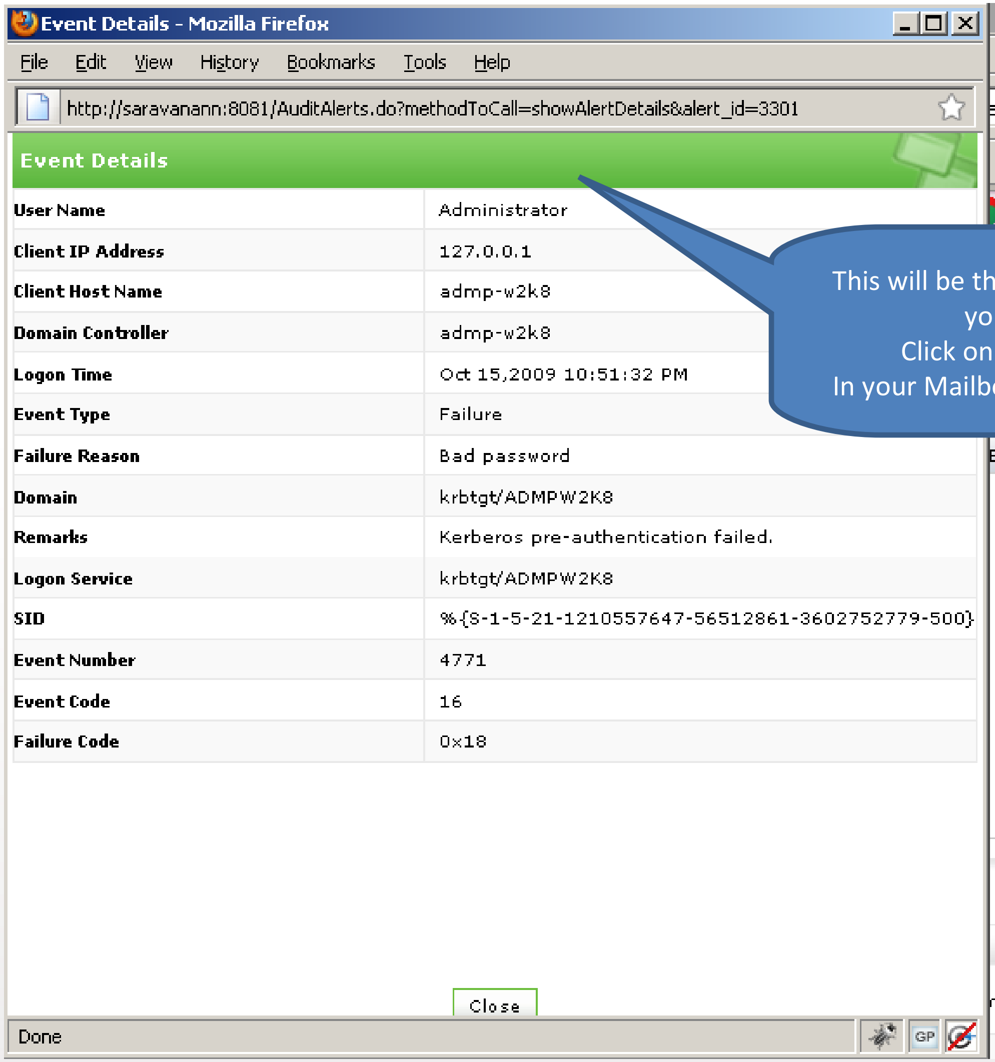
☐	Source	Domain	Severity	Alert Message	Time Generated
☐	emp-dc2	child	Attention	Login failure for User 'Administrator' in 'emp-dc2'. Reason: 'Bad password'.	Mar 08,2009 03:41:20 PM
☐	emp-dc2	child	Attention	Login failure for User 'Administrator' in 'emp-dc2'. Reason: 'Bad password'.	Mar 08,2009 03:41:16 PM
☐	emp-dc2	child	Attention	Login failure for User 'Administrator' in 'emp-dc1.zohocorpin.com'. Reason: 'Bad password'.	Mar 07,2009 02:33:21 PM
☐	emp-dc2	child	Attention	Login failure for User 'Administrator' in 'emp-dc1.zohocorpin.com'.	Mar 07,2009 09:44:20 AM

Removes the alert in totality

Removes the alerted event from Active Alerts. You can still view them under “All alerts”

Click on the alert to view complete data for the change event.(See next page)

What event detail does each alert provide.

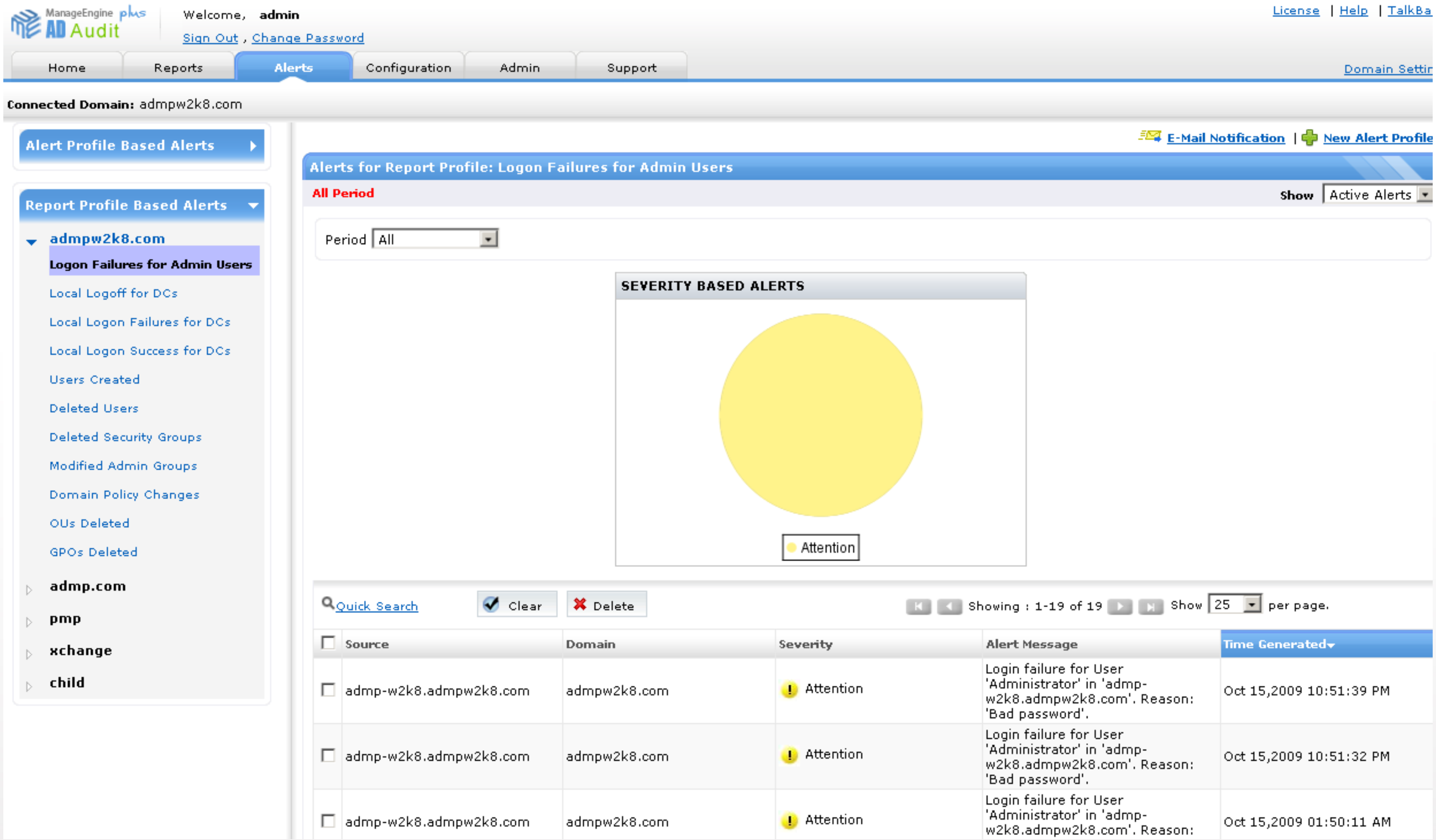

Event Details - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://saravanann:8081/AuditAlerts.do?methodToCall=showAlertDetails&alert_id=3301
Close
Done

Event Details

User Name	Administrator
Client IP Address	127.0.0.1
Client Host Name	admp-w2k8
Domain Controller	admp-w2k8
Logon Time	Oct 15,2009 10:51:32 PM
Event Type	Failure
Failure Reason	Bad password
Domain	krbtgt/ADMPW2K8
Remarks	Kerberos pre-authentication failed.
Logon Service	krbtgt/ADMPW2K8
SID	%{S-1-5-21-1210557647-56512861-3602752779-500}
Event Number	4771
Event Code	16
Failure Code	0x18

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.

Report Profile Based Alert


ManageEngine ADAudit Plus
Home
Reports
Alerts
Configuration
Admin
Support
License | Help | TalkBa
Domain Settir
Sign Out , Change Password
E-Mail Notification | New Alert Profile
Alert Profile Based Alerts
Report Profile Based Alerts
SEVERITY BASED ALERTS
Attention
Quick Search
Clear
Delete

Welcome, admin

Connected Domain: admpw2k8.com

- admpw2k8.com
  - Logon Failures for Admin Users
  - Local Logoff for DCs
  - Local Logon Failures for DCs
  - Local Logon Success for DCs
  - Users Created
  - Deleted Users
  - Deleted Security Groups
  - Modified Admin Groups
  - Domain Policy Changes
  - OUs Deleted
  - GPOs Deleted
- admp.com
- pmp
- xchange
- child

Alerts for Report Profile: Logon Failures for Admin Users

All Period

Show Active Alerts

Period All

Showing : 1-19 of 19 Show 25 per page.

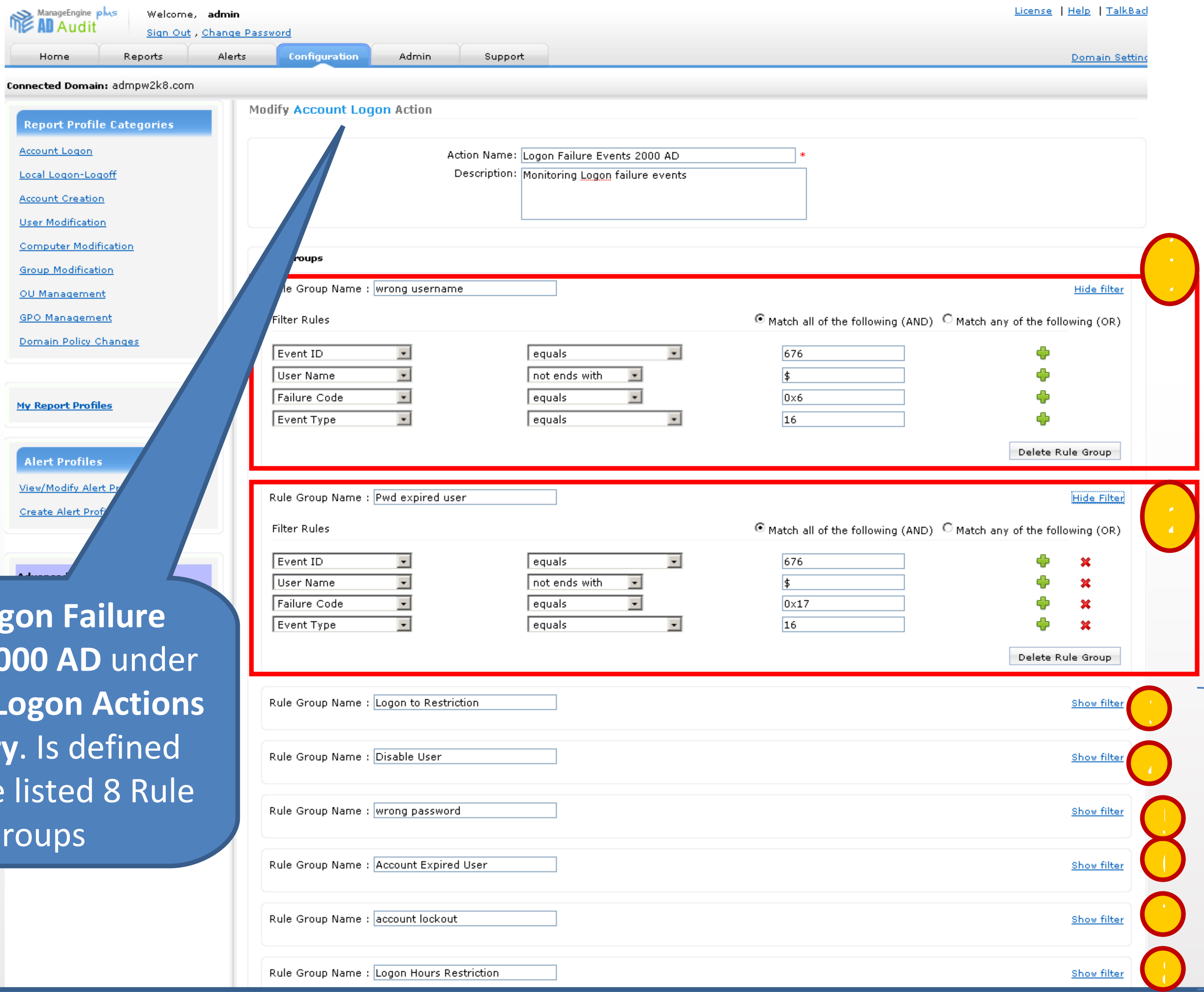
□	Source	Domain	Severity	Alert Message	Time Generated
□	admp-w2k8.admpw2k8.com	admpw2k8.com	Attention	Login failure for User 'Administrator' in 'admp-w2k8.admpw2k8.com'. Reason: 'Bad password'.	Oct 15,2009 10:51:39 PM
□	admp-w2k8.admpw2k8.com	admpw2k8.com	Attention	Login failure for User 'Administrator' in 'admp-w2k8.admpw2k8.com'. Reason: 'Bad password'.	Oct 15,2009 10:51:32 PM
□	admp-w2k8.admpw2k8.com	admpw2k8.com	Attention	Login failure for User 'Administrator' in 'admp-w2k8.admpw2k8.com'. Reason:	Oct 15,2009 01:50:11 AM

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



Connected Domain: admpw2k8.com

Modify Account Logon Action

Action Name: Logon Failure Events 2000 AD *

Description: Monitoring Logon failure events

roups

Rule Group Name : wrong username — Hide filter

Filter Rules ● Match all of the following (AND) ○ Match any of the following (OR)

Event ID	equals	676
User Name	not ends with	$
Failure Code	equals	0x6
Event Type	equals	16

Delete Rule Group

Rule Group Name : Pwd expired user — Hide Filter

Filter Rules ● Match all of the following (AND) ○ Match any of the following (OR)

Event ID	equals	676
User Name	not ends with	$
Failure Code	equals	0x17
Event Type	equals	16

Delete Rule Group

Rule Group Name : Logon to Restriction — Show filter

Rule Group Name : Disable User — Show filter

Rule Group Name : wrong password — Show filter

Rule Group Name : Account Expired User — Show filter

Rule Group Name : account lockout — Show filter

Rule Group Name : Logon Hours Restriction — Show filter

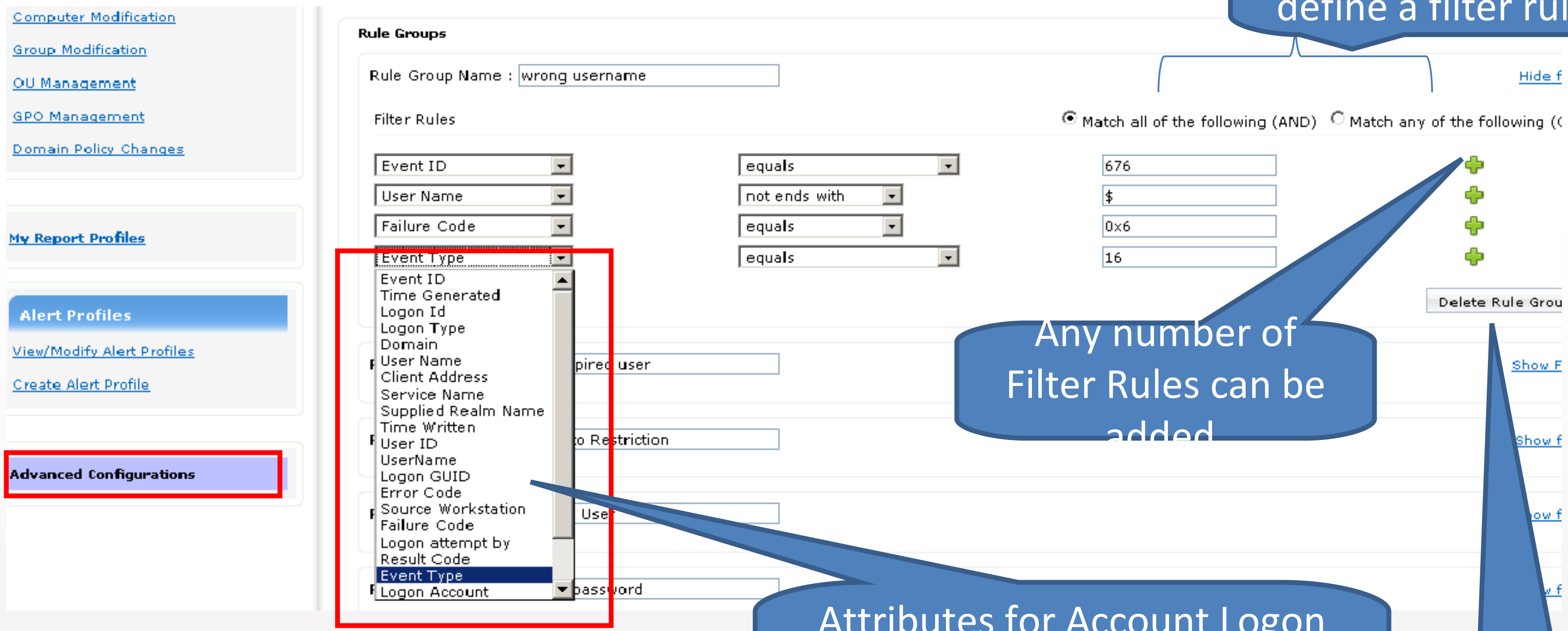
The Logon Failure events 2000 AD under **Account Logon Actions Category**. Is defined using the listed 8 Rule Groups

Filter Rules Shown

Filter Rules hidden

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

Advanced Configuration - A Rule Group Explained



Computer Modification

Group Modification

OU Management

GPO Management

Domain Policy Changes

My Report Profiles

Alert Profiles

View/Modify Alert Profiles

Create Alert Profile

Advanced Configurations

Rule Groups

Rule Group Name : wrong username

Hide f

Filter Rules

● Match all of the following (AND) ○ Match any of the following (

Event ID	equals	676
User Name	not ends with	$
Failure Code	equals	0x6
Event Type	equals	16

Event ID
Time Generated
Logon Id
Logon Type
Domain
User Name
Client Address
Service Name
Supplied Realm Name
Time Written
User ID
UserName
Logon GUID
Error Code
Source Workstation
Failure Code
Logon attempt by
Result Code
Event Type
Logon Account

Delete Rule Grou

pired user

o Restriction

Use

password

Show F

Show f

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.

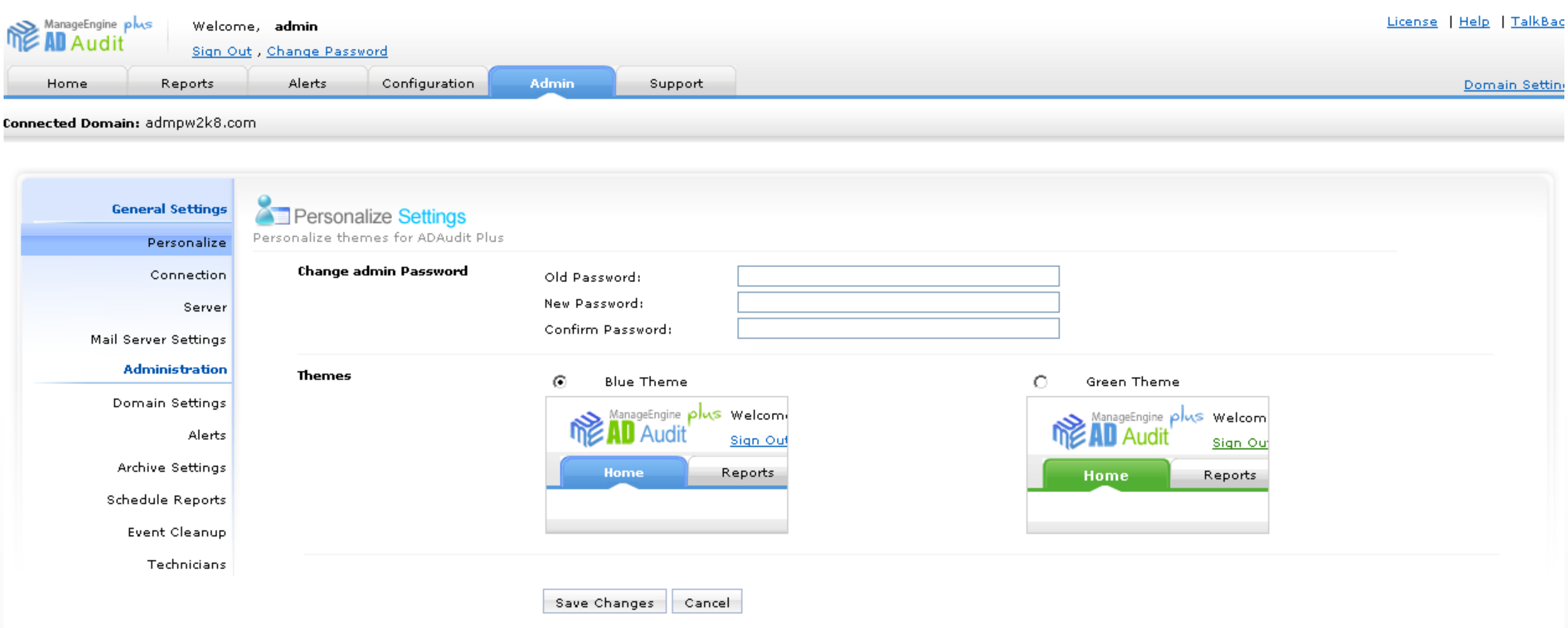
Admin Tab

Admin Tab of ADAudit Plus

Admin Tab

- The Admin tab of ADAudit Plus allows you to configure the various settings for working with the product.

Personalize Tab



Connected Domain: admpw2k8.com

Personalize Settings

Personalize themes for ADAudit Plus

Change admin Password

Old Password:

New Password:

Confirm Password:

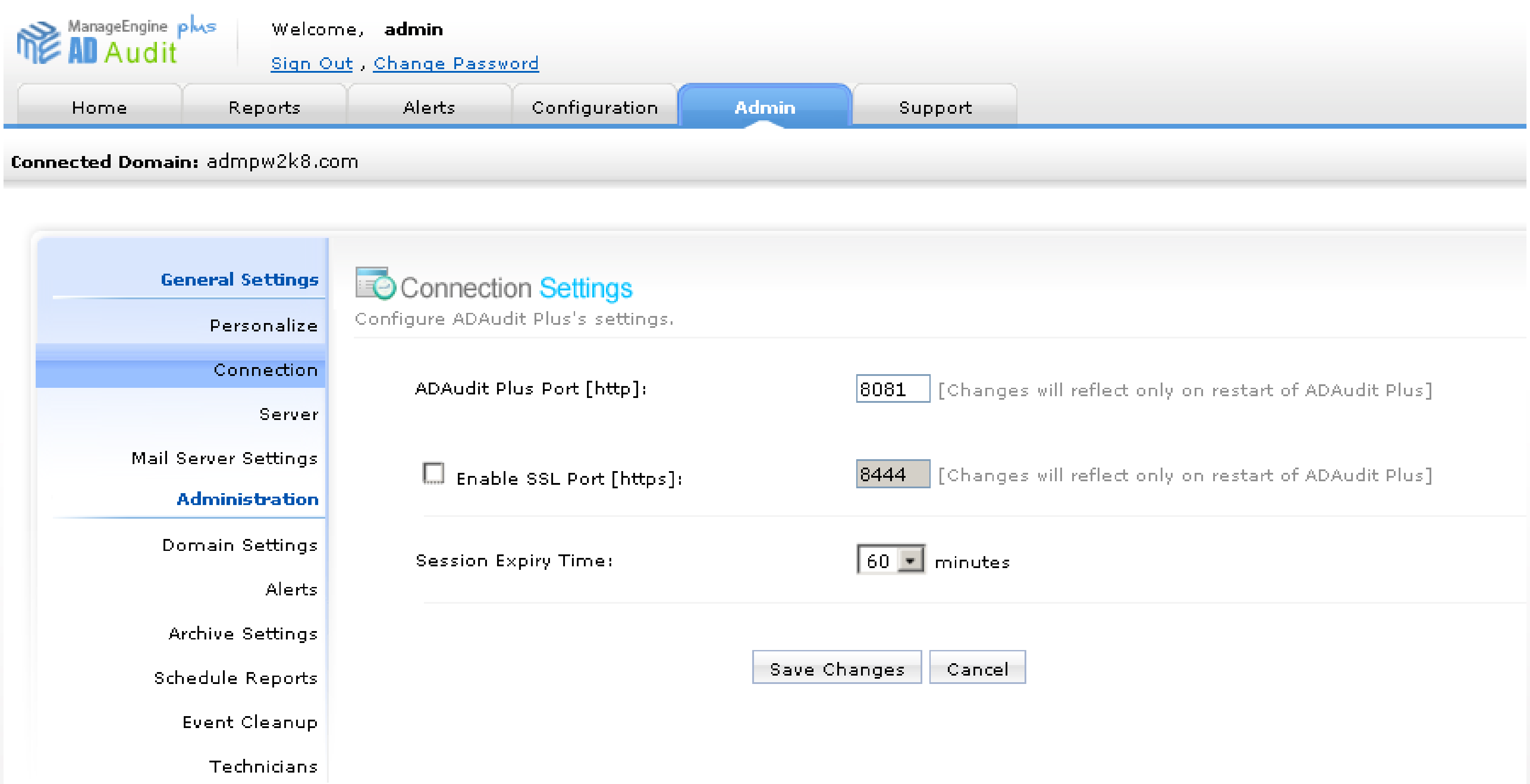
Themes

● Blue Theme

○ Green Theme

This Tab allows you to personalize ADAudit Plus by selecting a theme and changing the default password to desired.

Connections



Welcome, **admin**

Sign Out , Change Password

Connected Domain: admpw2k8.com

Connection Settings

Configure ADAudit Plus's settings.

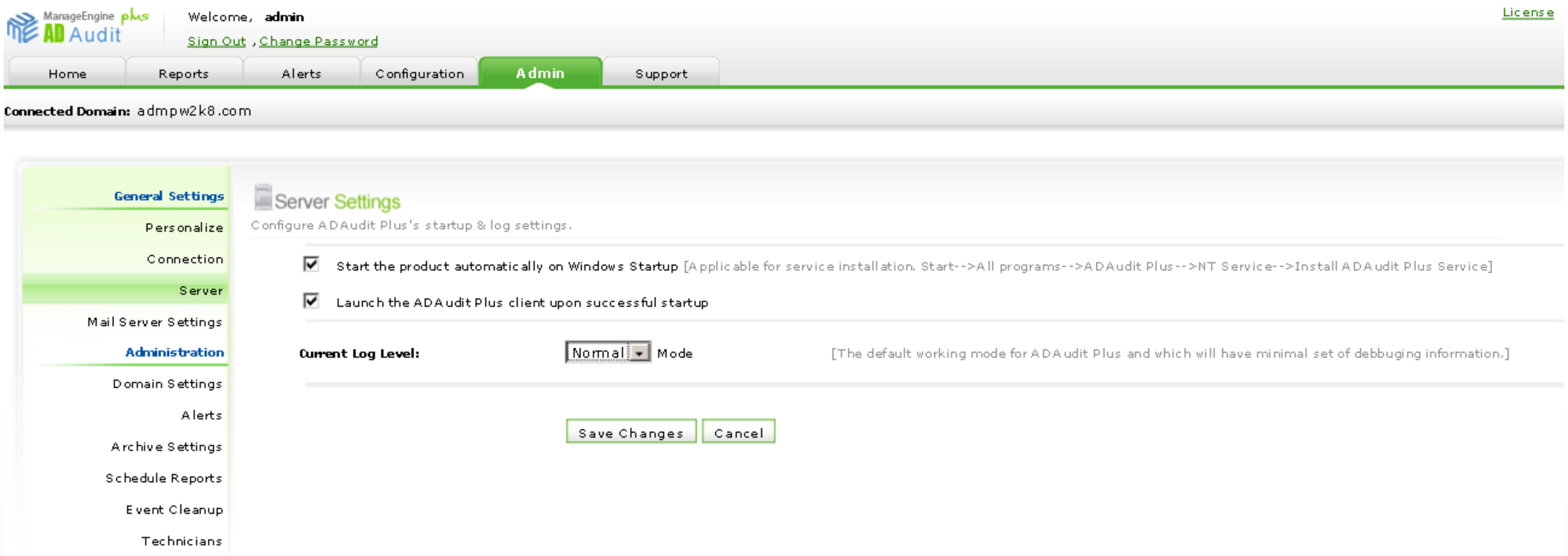
ADAudit Plus Port [http]: 8081 [Changes will reflect only on restart of ADAudit Plus]

□ Enable SSL Port [https]: 8444 [Changes will reflect only on restart of ADAudit Plus]

Session Expiry Time: 60 minutes

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.

Server Settings



Connected Domain: admpw2k8.com

Server Settings

Configure ADAudit Plus's startup & log settings.

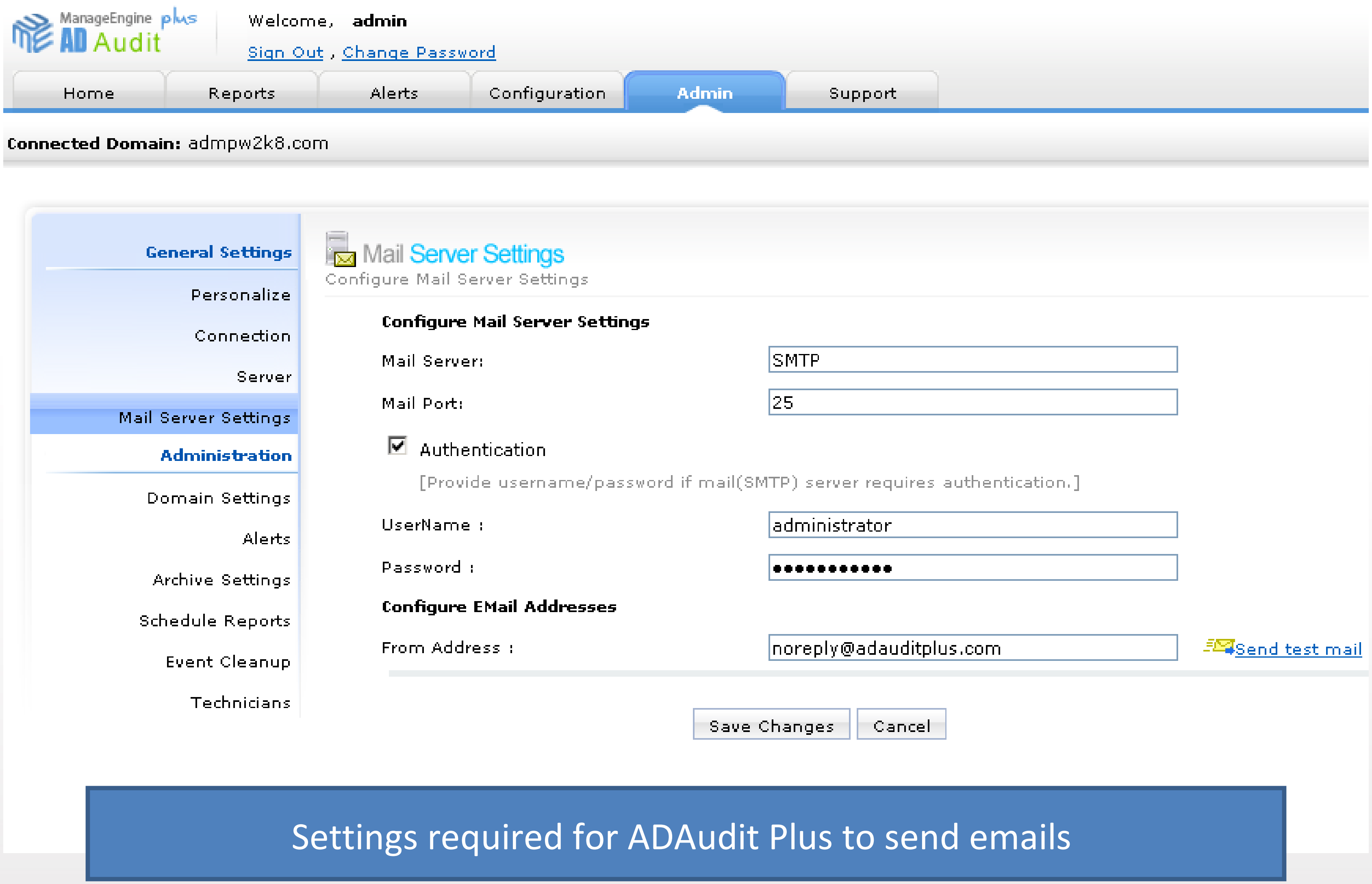
☑ Start the product automatically on Windows Startup [Applicable for service installation. Start-->All programs-->ADAudit Plus-->NT Service-->Install ADAudit Plus Service]

☑ Launch the ADAudit Plus client upon successful startup

Current Log Level: Normal Mode [The default working mode for ADAudit Plus and which will have minimal set of debbuging information.]

Settings required for ADAudit Plus to start and for debugging can be set in this Tab.

Mail Server Settings



Connected Domain: admpw2k8.com

Mail Server Settings

Configure Mail Server Settings

Configure Mail Server Settings

Mail Server: SMTP

Mail Port: 25

☑ Authentication

[Provide username/password if mail(SMTP) server requires authentication.]

UserName : administrator

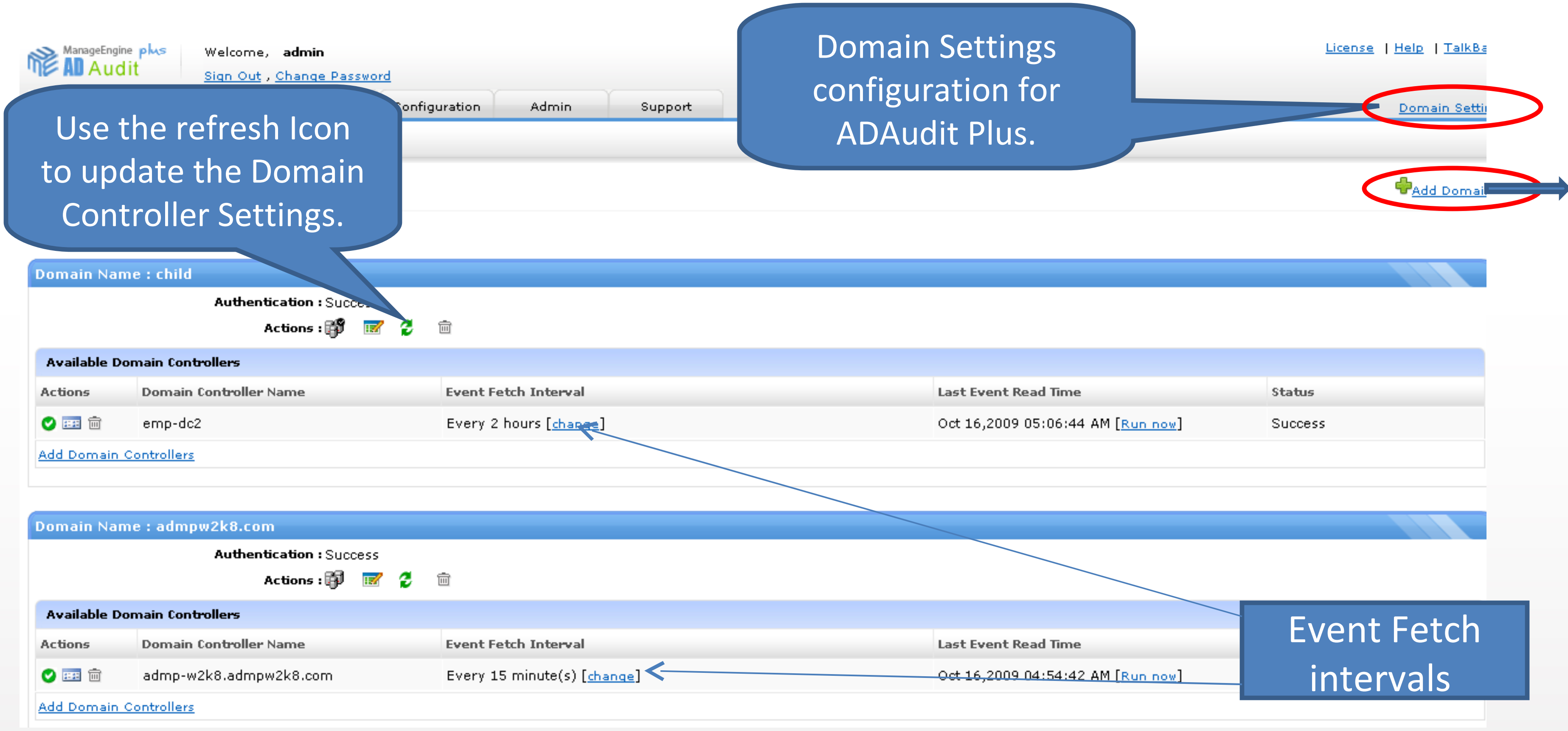
Password : ●●●●●●●●●●●

Configure EMail Addresses

From Address : noreply@adauditplus.com

Settings required for ADAudit Plus to send emails

Domain Settings



ManageEngine plus AD Audit

Welcome, **admin**

Sign Out , Change Password

License | Help | TalkBa

Domain Settings configuration for ADAudit Plus.

Use the refresh Icon to update the Domain Controller Settings.

Event Fetch intervals

Domain Name : child

Authentication : Succe

Actions :

Available Domain Controllers

Actions	Domain Controller Name	Event Fetch Interval	Last Event Read Time	Status
✓	emp-dc2	Every 2 hours [change]	Oct 16,2009 05:06:44 AM [Run now]	Success

Add Domain Controllers

Domain Name : admpw2k8.com

Authentication : Success

Actions :

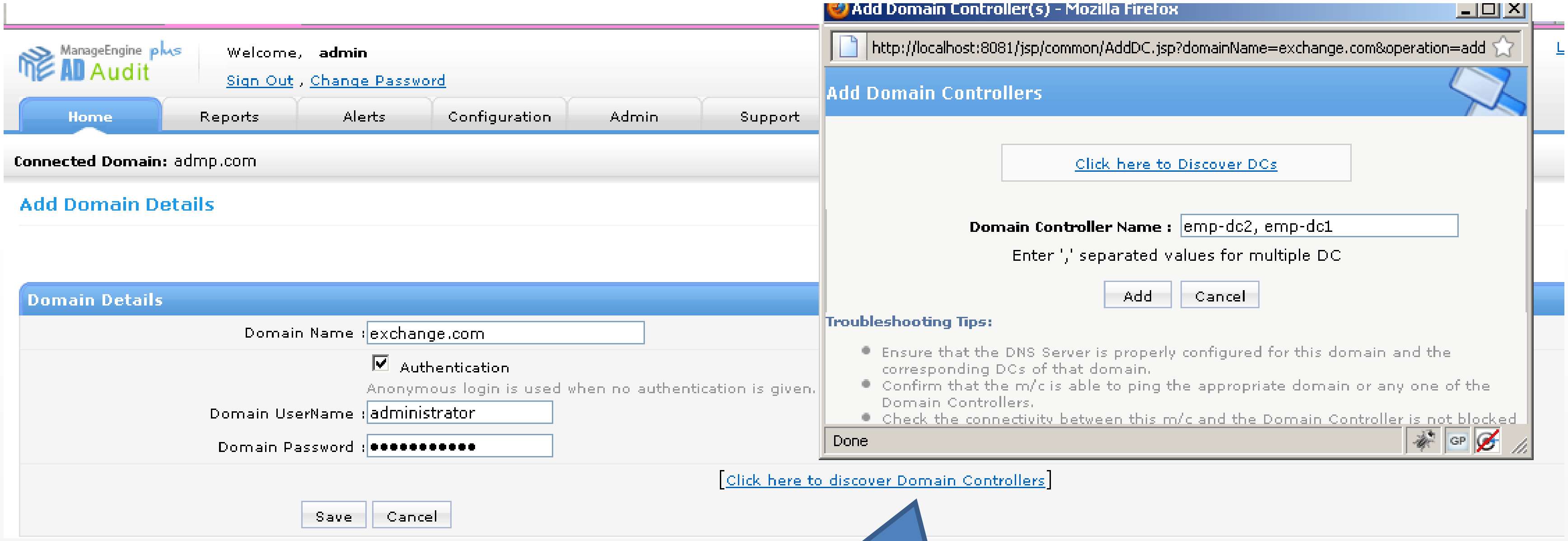
Available Domain Controllers

Actions	Domain Controller Name	Event Fetch Interval	Last Event Read Time
✓	admp-w2k8.admpw2k8.com	Every 15 minute(s) [change]	Oct 16,2009 04:54:42 AM [Run now]

Add Domain Controllers

- 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



Welcome, **admin**

Sign Out , Change Password

Connected Domain: admp.com

Add Domain Details

Domain Details

Domain Name : exchange.com

☑ Authentication

Anonymous login is used when no authentication is given.

Domain UserName : administrator

Domain Password : ●●●●●●●●●●●●

[Click here to discover Domain Controllers]

Save   Cancel

Add Domain Controller(s) - Mozilla Firefox

http://localhost:8081/jsp/common/AddDC.jsp?domainName=exchange.com&operation=add

Add Domain Controllers

Click here to Discover DCs

Domain Controller Name : emp-dc2, emp-dc1

Enter ',' separated values for multiple DC

Add   Cancel

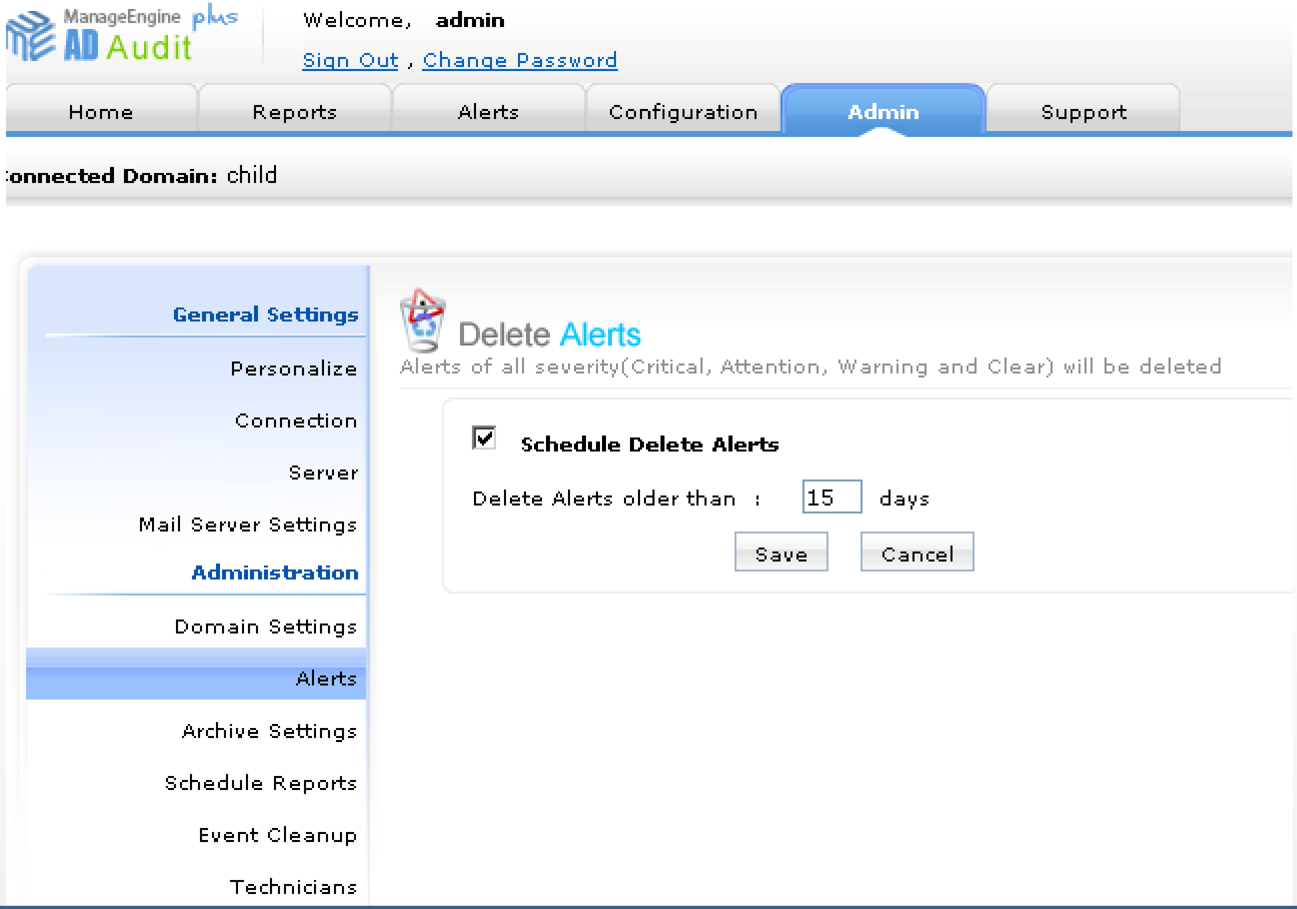
Troubleshooting Tips:

- Ensure that the DNS Server is properly configured for this domain and the corresponding DCs of that domain.
- Confirm that the m/c is able to ping the appropriate domain or any one of the Domain Controllers.
- Check the connectivity between this m/c and the Domain Controller is not blocked

Done

Adding a Domain controller. Multiple DC's added by separating them using comma

Schedule Deletion of Alerts



:onnected Domain: child

Delete Alerts

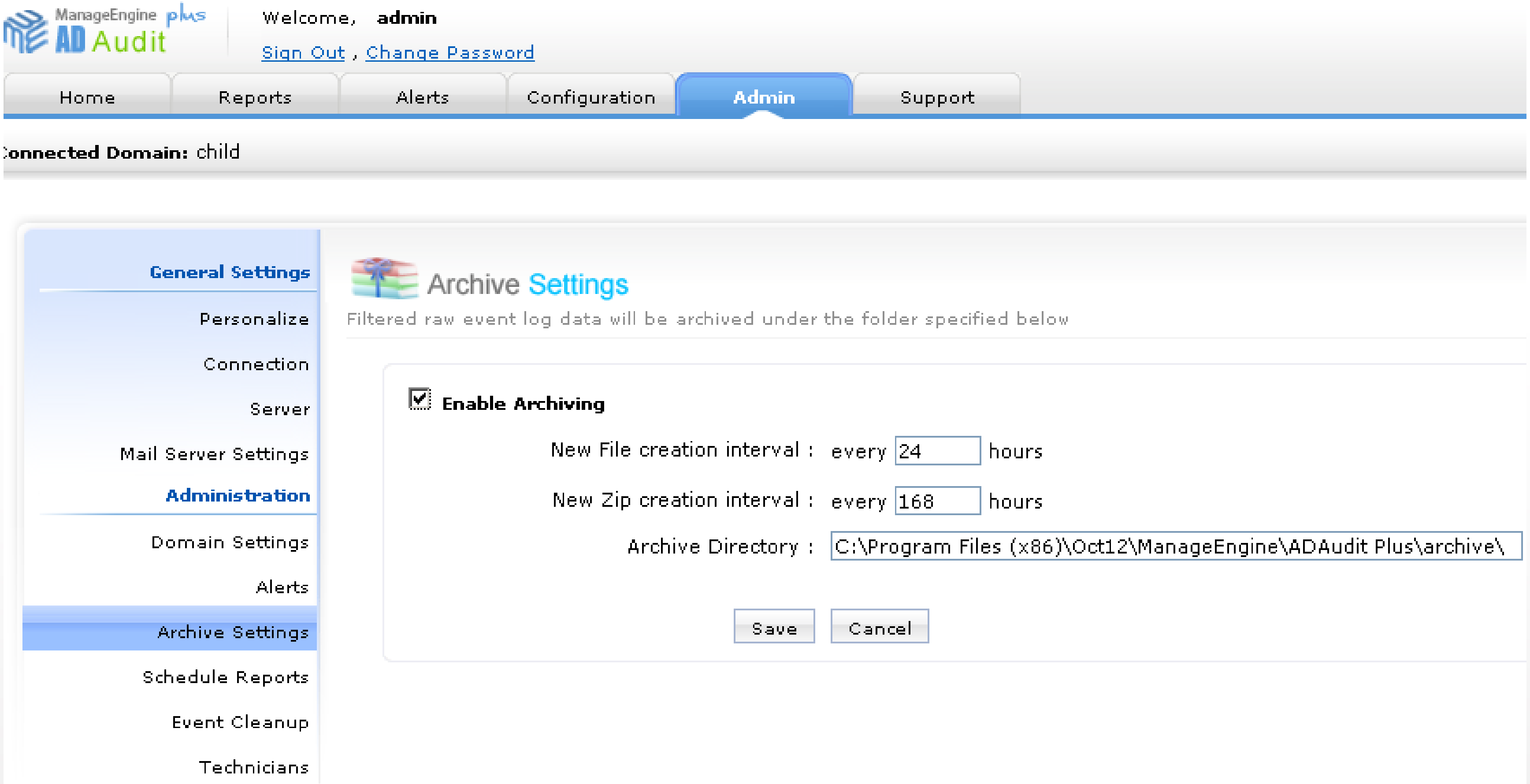
Alerts of all severity(Critical, Attention, Warning and Clear) will be deleted

☑ Schedule Delete Alerts

Delete Alerts older than : 15 days

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



:onnected Domain: child

Archive Settings

Filtered raw event log data will be archived under the folder specified below

☑ Enable Archiving

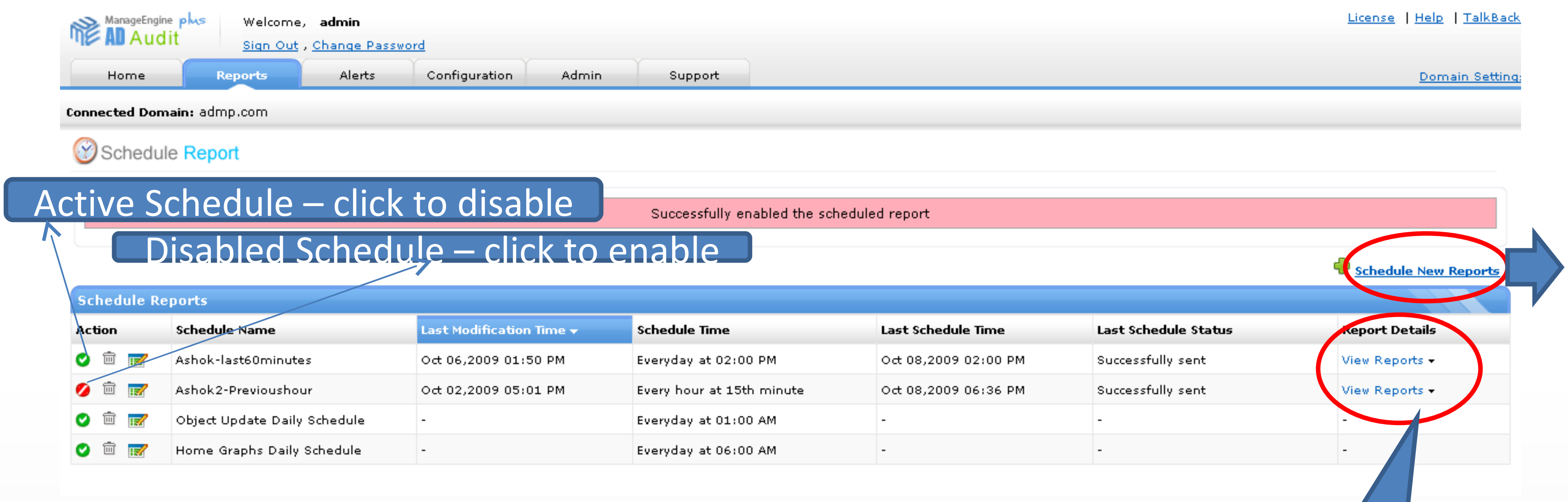
New File creation interval : every 24 hours

New Zip creation interval : every 168 hours

Archive Directory : C:\Program Files (x86)\Oct12\ManageEngine\ADAudit Plus\archive\

Filtered raw eventlog data are archived under the folder mentioned. The time and folders are configured here.

Scheduled Reports



ManageEngine plus AD Audit

Welcome, **admin**

Sign Out , Change Password

License | Help | TalkBack

Connected Domain: admp.com

Schedule Report

Active Schedule – click to disable

Successfully enabled the scheduled report

Disabled Schedule – click to enable

Schedule New Reports

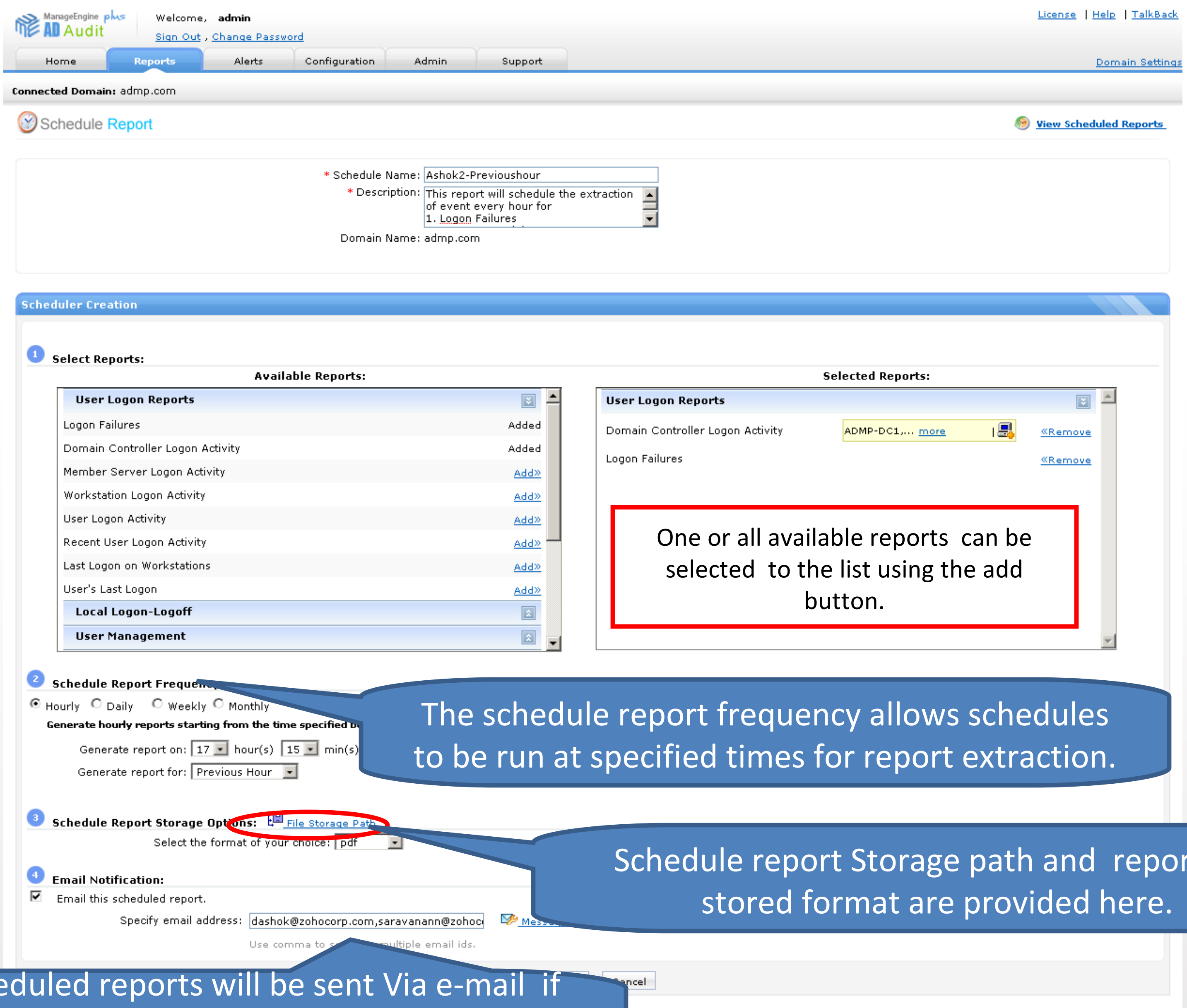
Schedule Reports

Action	Schedule Name	Last Modification Time ▾	Schedule Time	Last Schedule Time	Last Schedule Status	Report Details
✓ 🗑 ✎	Ashok-last60minutes	Oct 06,2009 01:50 PM	Everyday at 02:00 PM	Oct 08,2009 02:00 PM	Successfully sent	View Reports ▾
⊘ 🗑 ✎	Ashok2-Previoushour	Oct 02,2009 05:01 PM	Every hour at 15th minute	Oct 08,2009 06:36 PM	Successfully sent	View Reports ▾
✓ 🗑 ✎	Object Update Daily Schedule	-	Everyday at 01:00 AM	-	-	-
✓ 🗑 ✎	Home Graphs Daily Schedule	-	Everyday at 06:00 AM	-	-	-

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

Viewing all Scheduled reports

Scheduling a Report



ManageEngine ADAudit Plus

Welcome, admin

Sign Out , Change Password

License | Help | TalkBack

Connected Domain: admp.com

Schedule Report

View Scheduled Reports

* Schedule Name: Ashok2-Previoushour

* Description: This report will schedule the extraction of event every hour for
1. Logon Failures

Domain Name: admp.com

Scheduler Creation

1 **Select Reports:**

Available Reports:	
User Logon Reports	
Logon Failures	Added
Domain Controller Logon Activity	Added
Member Server Logon Activity	Add»
Workstation Logon Activity	Add»
User Logon Activity	Add»
Recent User Logon Activity	Add»
Last Logon on Workstations	Add»
User's Last Logon	Add»
Local Logon-Logoff	
User Management	

Selected Reports:		
User Logon Reports		
Domain Controller Logon Activity	ADMP-DC1,... more	«Remove
Logon Failures		«Remove

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

2 **Schedule Report Frequen**

● Hourly ○ Daily ○ Weekly ○ Monthly

Generate hourly reports starting from the time specified b

Generate report on: 17 hour(s) 15 min(s)

Generate report for: Previous Hour

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

3 **Schedule Report Storage Options:** File Storage Path

Select the format of your choice: pdf

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

4 **Email Notification:**

☑ Email this scheduled report.

Specify email address: dashok@zohocorp.com,saravanann@zohoc

Mes

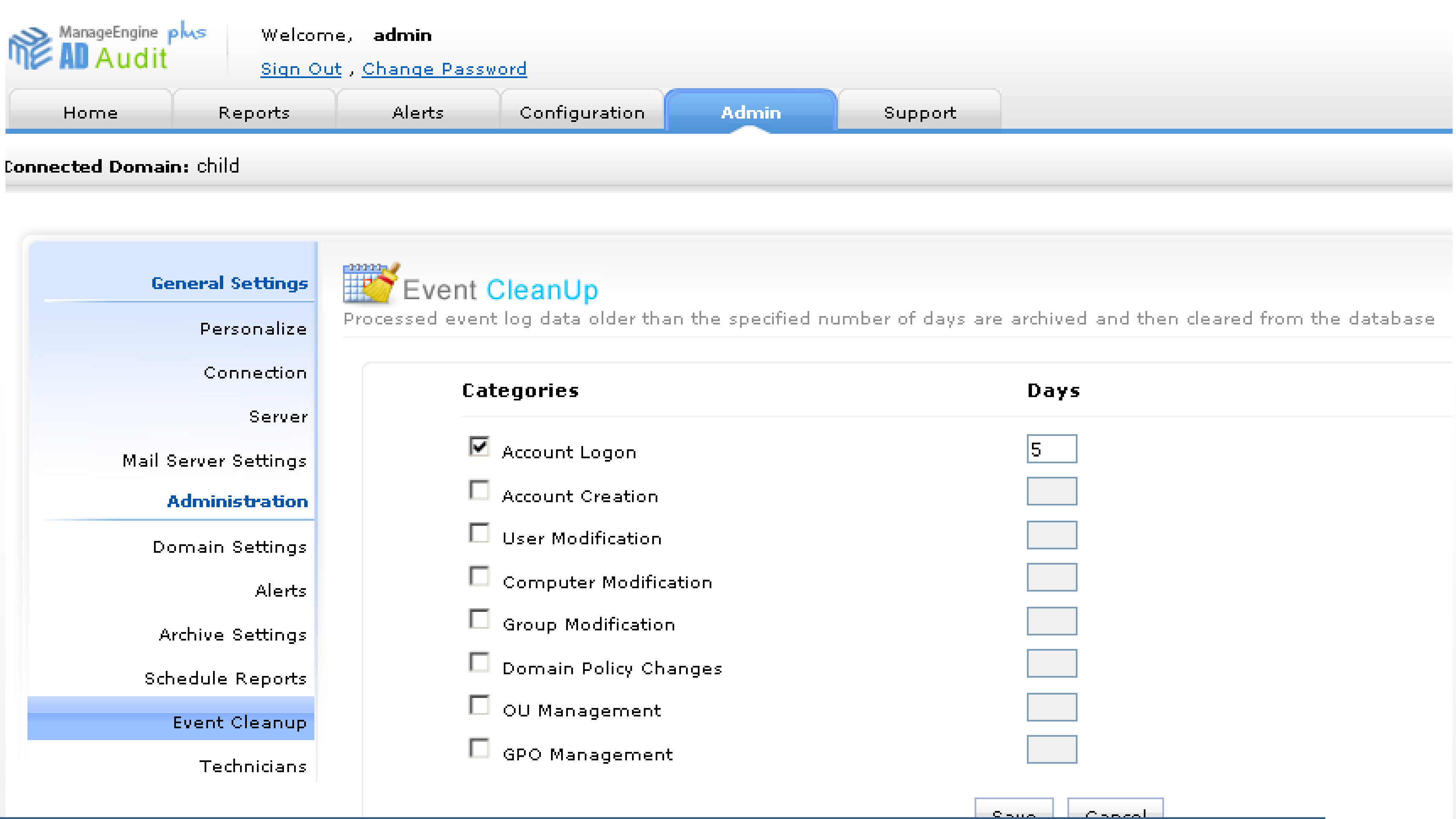
Use comma to s multiple email ids.

ncel

The scheduled reports will be sent Via e-mail if this option is checked. And for the configured settings.

ManageEngine

Event CleanUp



Connected Domain: child

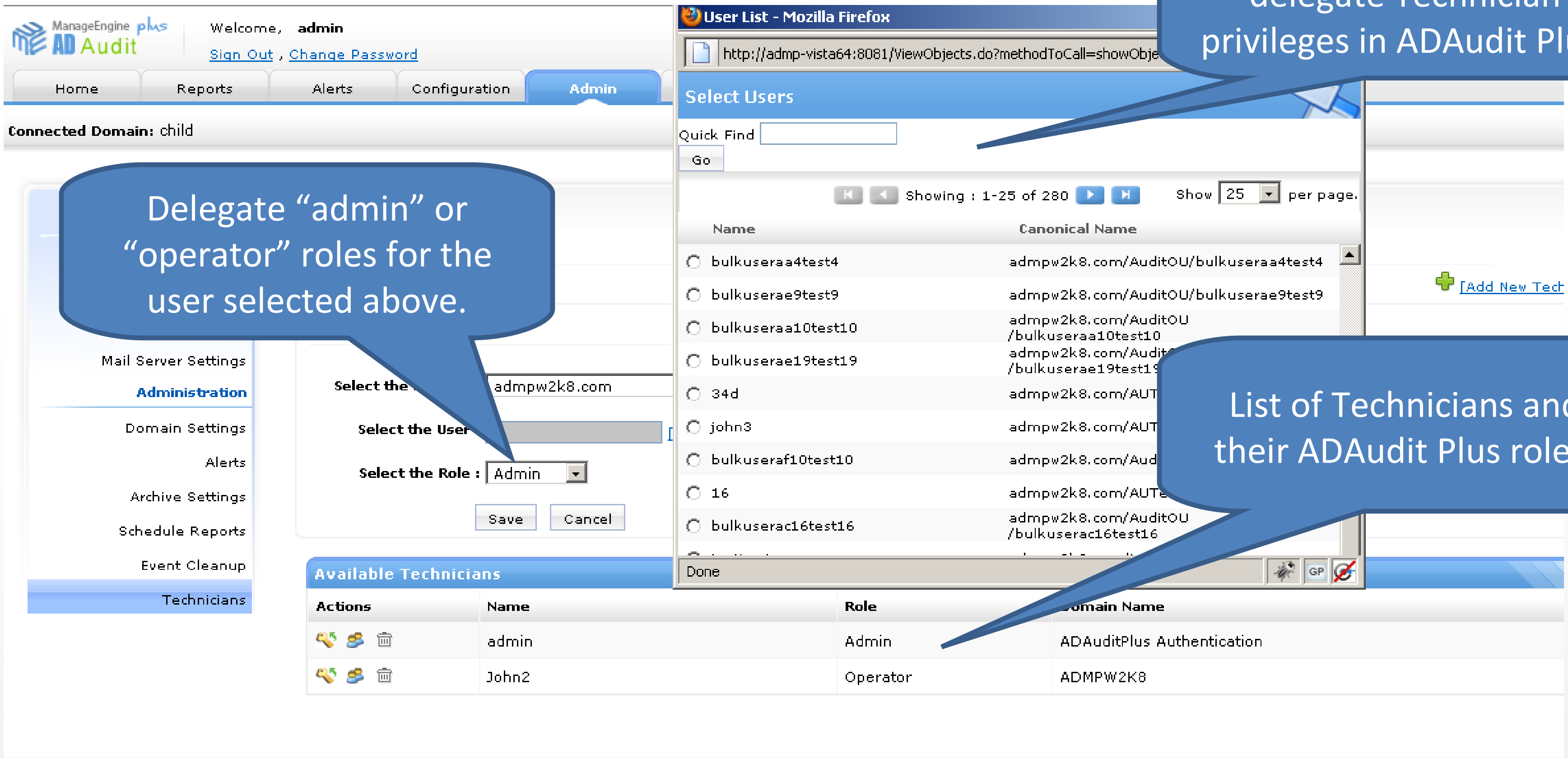
Event CleanUp

Processed event log data older than the specified number of days are archived and then cleared from the database

Categories	Days
☑ Account Logon	5
□ Account Creation	
□ User Modification	
□ Computer Modification	
□ Group Modification	
□ Domain Policy Changes	
□ OU Management	
□ GPO Management	

Processed eventlog 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.

Technicians



Welcome, **admin**

Sign Out , Change Password

Connected Domain: child

Select the : admpw2k8.com

Select the User

Select the Role : Admin

http://admp-vista64:8081/ViewObjects.do?methodToCall=showObje

Select Users

Quick Find

Showing : 1-25 of 280 Show 25 per page.

Name	Canonical Name
○ bulkuseraa4test4	admpw2k8.com/AuditOU/bulkuseraa4test4
○ bulkuserae9test9	admpw2k8.com/AuditOU/bulkuserae9test9
○ bulkuseraa10test10	admpw2k8.com/AuditOU /bulkuseraa10test10
○ bulkuserae19test19	admpw2k8.com/Audit /bulkuserae19test19
○ 34d	admpw2k8.com/AUT
○ john3	admpw2k8.com/AUT
○ bulkuseraf10test10	admpw2k8.com/Aud
○ 16	admpw2k8.com/AUTE
○ bulkuserac16test16	admpw2k8.com/AuditOU /bulkuserac16test16

Available Technicians

Actions	Name	Role	Domain Name
	admin	Admin	ADAuditPlus Authentication
	John2	Operator	ADMPW2K8

Select any user do delegate Technician privileges in ADAudit Plus.

Delegate “admin” or “operator” roles for the user selected above.

List of Technicians and their ADAudit Plus roles.

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