User Manual

Active Directory Change Tracker

Active Directory Change Tracker

Change Auditing, Tracking and Analysis for Active Directory

Copyright © 2011-2022 Vyapin Software Systems Private Limited. All Rights Reserved.

Email: support@vyapin.com Web: www.vyapin.com

Last Updated: June 2022

Vyapin Software Systems Private Limited

Website: http://www.vyapin.com/
Sales Contact: sales@vyapin.com
Technical Support: support@vyapin.com

Table of Contents

1 General

1.1 About Vyapin Active Directory Change Tracker (ADChangeTracker)

Vyapin Active Directory Change Tracker (ADChangeTracker) audits, tracks and analyzes all changes made to your Active Directory configuration. The tool audits all changes made to your Active Directory by periodically collecting only the changed data, reporting what exactly changed, along with the new and old values, when the change was made, where the change happened in your Active Directory and the tool also determines who made the change by looking up the Security Event logs of your audit enabled Active Directory.. Active Directory Change tracker records and maintains the entire history all tracked changes along with the relevant Event log data in a SQL server database for future reference and analysis. A powerful search tool helps you analyze all past changes on any predefined search criteria. Changes can be selectively tracked (such as only OUs) and a powerful email notification mechanism lets you configure different types of changes (such as Created, Deleted, and Modified) and get them notified to different end users based on the OUs/containers where the changes happened.

1.2 System Requirements

For the computer running ADChangeTracker

Processor Intel Pentium Processor

Disk Space & Memory 512 MB RAM and minimum of 20 MB of free disk space

Operating System

Windows 10 / Windows 8.1 / Windows 8 / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 with .NET Framework 4.0 or higher with the latest service packs.

Database

Microsoft SQL Server 2012 (Enterprise / Standard / Developer / Express edition) or Microsoft SQL Server 2008 (Enterprise / Standard / Developer / Express edition) running in local / remote computer with latest Service Pack.

Software MDAC v2.5/2.6/2.8

For the computers reported by ADChangeTracker

Windows Server 2012 R2 / Windows Server 2012 / Windows Server 2008 R2 / Windows Server 2008 running Active Directory.

1.3 Who can Use ADChangeTracker?

Organizations running Microsoft Active Directory can greatly benefit from ADChangeTracker. It is a powerful Change auditing tool for Active Directory Administrators. System Administrators can monitor changes to Active Directory Servers across the enterprise network in any location.

Users that would benefit from ADChangeTracker:

- Systems management personnel
- CIOs and CSOs
- Security and Systems Audit personnel
- System Administrators

Organizations that would benefit from ADChangeTracker:

- Companies having enterprise network based on Active Directory
- Any company having Windows 2012 R2 / 2012 / 2008 R2 / 2008 Active Directory servers

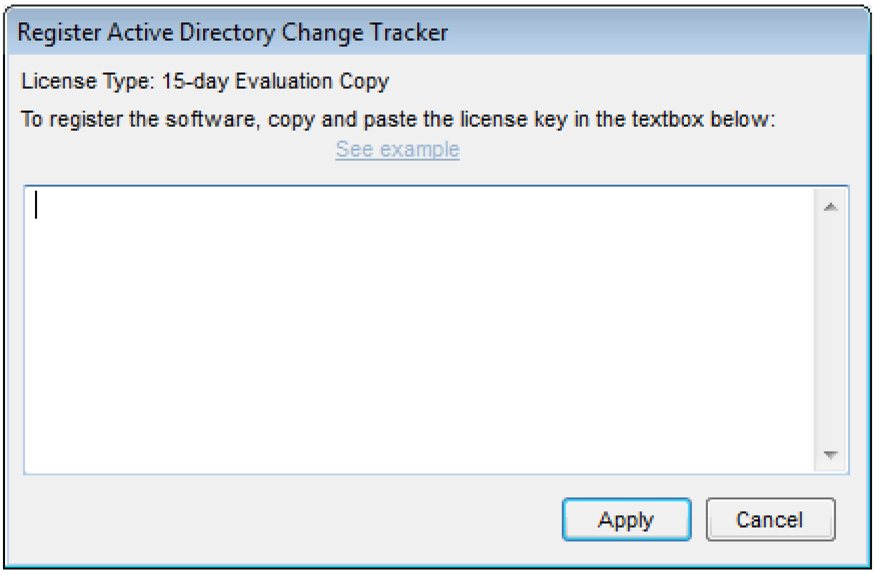
1.4 How to Register the Software?

Once you purchase the software online or through any one of our resellers, you will receive a sale notification through e-mail from our sales department. We will send you an e-mail with the necessary instructions to activate the software.

In case you do not receive an e-mail from our sales team after you purchase the software, please send the following information to our sales department at sales@vyapin.com with the sales order number:

- **Company Name:** End-user Company Name
- **Location:** City & Country for the Company Name given above

Please allow 12 to 24 hours from the time of purchase for our sales department to process your orders.



Register Active Directory Change Tracker

License Type: 15-day Evaluation Copy

To register the software, copy and paste the license key in the textbox below:

Image 1 - Activate screen

Perform the following steps to activate the software:

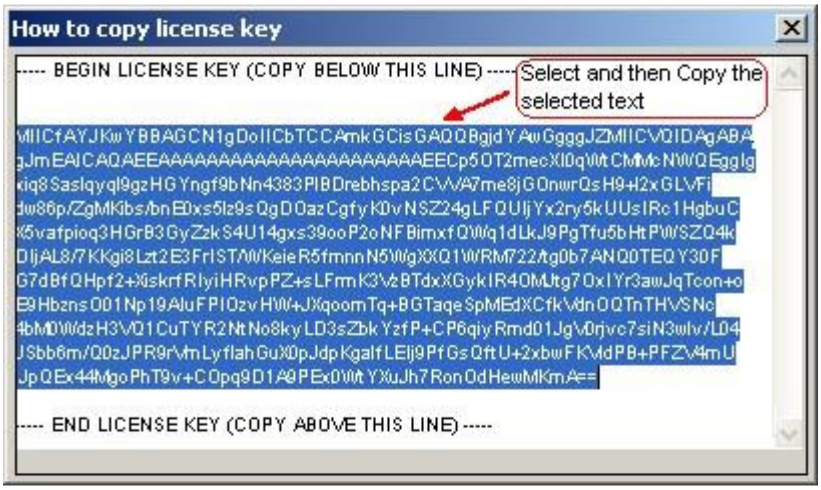
1) *Download evaluation*/trial copy of software from the respective product page available in our website at http://www.vyapin.com/

2) *Install* the software on the desired computer.

3) You will receive a *license key* through e-mail as soon as the purchase process is complete. You can also request the license key by using the “Request license key…” button in “About” dialog.

4) *Click 'Apply'* in *Help -> About ADChangeTracker ->Register license Key* button to see the Register dialog (as shown in Image 1).

5) *Copy the license key* sent to you through email and pastes it in the *'License Key' textbox.* For help on how to copy the license key, click 'See example' link in the Register dialog (as shown in Image 2).



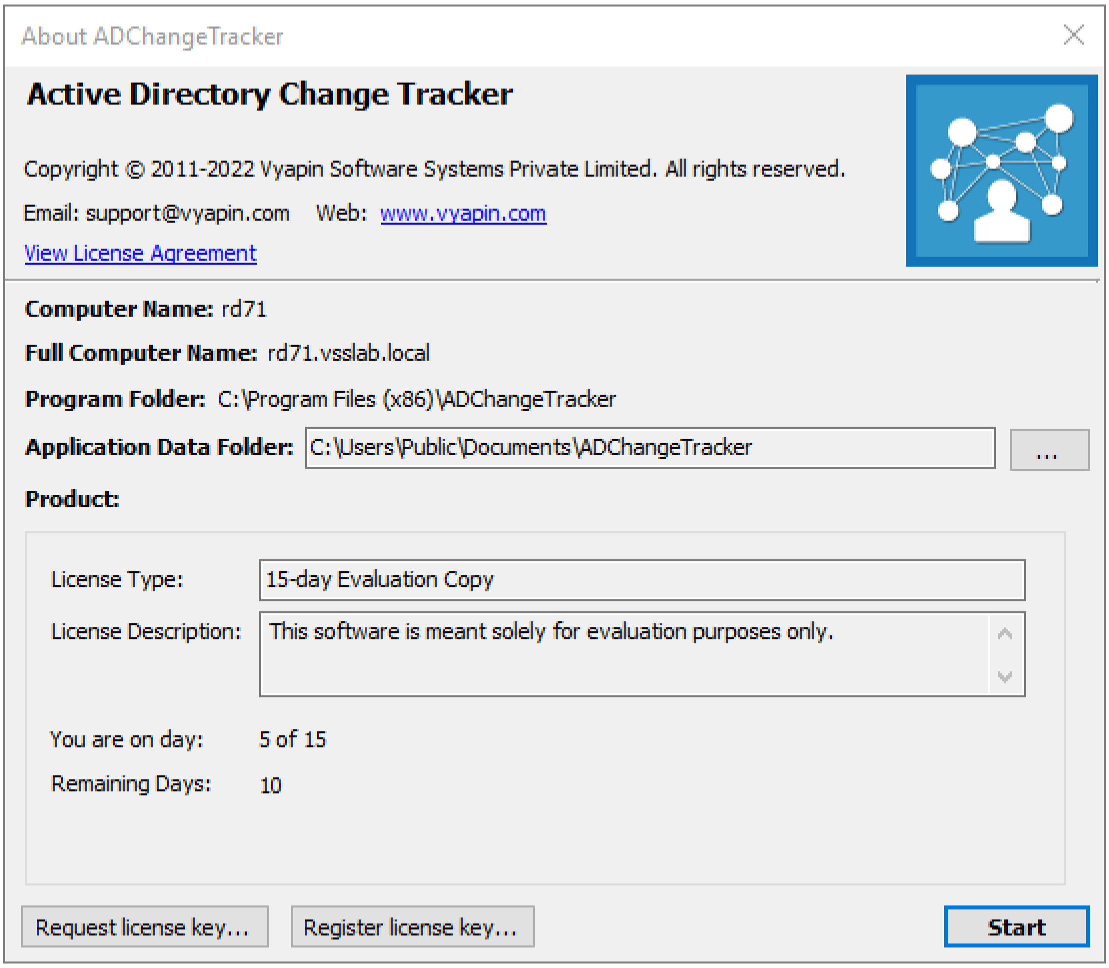
```
---- BEGIN LICENSE KEY (COPY BELOW THIS LINE) -----
MIICfAYJKwYBBAGCN1gDoIICbTCCAmkGCisGAQQBgjdYAwGgggJZMIICVQIDAgABA
gJmEAICAQAEEAAAAAAAAAAAAAAAAAAAAAAAEECp5OT2mecXI0qWtCMMcNWQEgglg
kiq8SaslqyqI9gzHGYngf9bNn4383PIBDrebhspa2CVVA7me8jGOnwrQsH9+l2xGLVFi
dw86p/ZgMKibs/bnE0xs5Iz9sQgDOazCgfyK0vNSZ24gLFQUIjYx2ry5kUUsIRc1HgbuC
X5vafpioq3HGrB3GyZzkS4U14gxs39ooP2oNFBimxfQWq1dLkJ9PgTfu5bHtPWSZQ4k
DIjAL8/7KKgi8Lzt2E3FrISTAWKeieR5fmnnN5WgXXQ1WRM722/tg0b7ANQ0TEQY30F
G7dBfQHpf2+XiskrfRIyiHRvpPZ+sLFmK3VzBTdxXGykIR4OMJtg7OxIYr3awJqTcon+o
E9HbznsO01Np19AluFPIOzvHW+JXqoomTq+BGTaqeSpMEdXCfkVdnOQTnTHVSNc
4bM0WdzH3VQ1CuTYR2NtNo8kyLD3sZbkYzfP+CP6qiyRmd01JgV0rjvc7siN3wlv/L04
JSbb6m/Q0zJPR9rVmLyflahGuX0pJdpKgalfLEIj9PfGsQftU+2xbwFKVdPB+PFZV4mU
JpQEx44MgoPhT9v+COpq9D1A9PEx0WtYXuJh7RonOdHewMKmA==

---- END LICENSE KEY (COPY ABOVE THIS LINE) -----
```

Image 2 - How to copy license key screen

Request License Key:

- Select *Help -> AboutADChangeTracker…* from toolbar.
- The *About ADChangeTracker dialog* will appear as shown below:



Active Directory Change Tracker

Copyright © 2011-2022 Vyapin Software Systems Private Limited. All rights reserved.

Email: support@vyapin.com   Web: www.vyapin.com

View License Agreement

Computer Name: rd71

Full Computer Name: rd71.vsslab.local

Program Folder: C:\Program Files (x86)\ADChangeTracker

Application Data Folder: C:\Users\Public\Documents\ADChangeTracker

Product:

License Type: 15-day Evaluation Copy

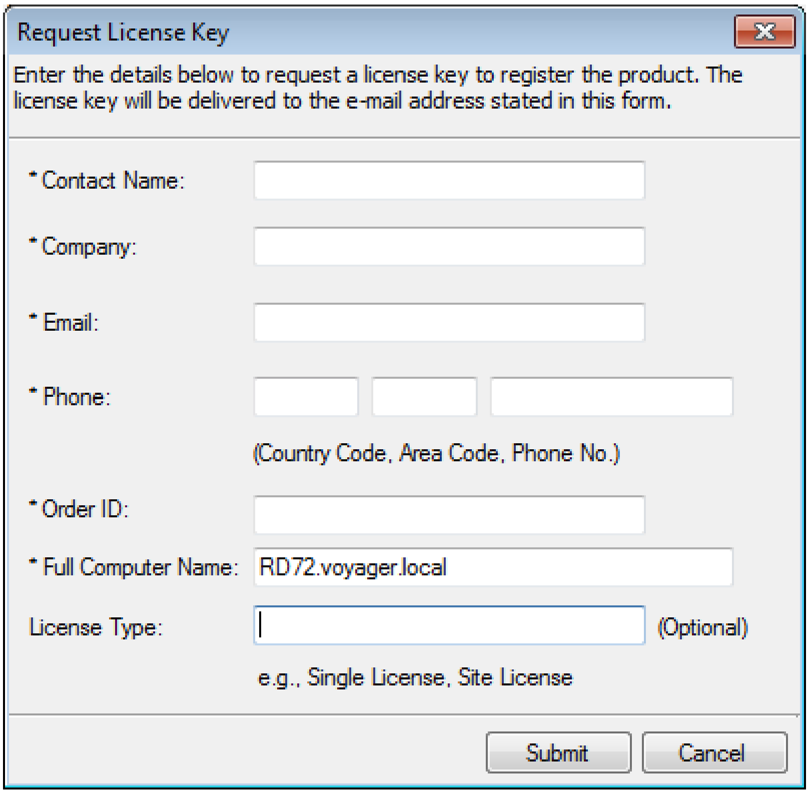
License Description: This software is meant solely for evaluation purposes only.

You are on day: 5 of 15

Remaining Days: 10

Image 3 - About screen

- Click **Request license key…** button. The Request License Key dialog will appear as shown below:



Request License Key

Enter the details below to request a license key to register the product. The license key will be delivered to the e-mail address stated in this form.

* Contact Name:

* Company:

* Email:

* Phone: (Country Code, Area Code, Phone No.)

* Order ID:

* Full Computer Name: RD72.voyager.local

License Type: (Optional)

e.g., Single License, Site License

Image 4 – Request License Key image

- Enter the following details and click Submit to place the license key request through email.
  - **Contact Name:** End-user of the product.
  - **Company:** End-user Company Name.
  - **Email:** Email address where the license key has to be sent.
  - **Phone:** Phone number with country code and area code.
  - **Order ID:** Order/Transaction ID reference.
  - **License Type:** License that was purchased.

2 Getting Started

2.1 Configure Active Directory Auditing

This section provides step-by-step procedures for enabling auditing of changes to objects in AD DS. This process consists of two primary steps:

- Step 1: Enable audit policy.
- Step 2: Set up auditing in object SACLs by using Active Directory Users and Computers console.

Step 1: Enable audit policy.

1) Click **Start**, point to **Administrative Tools**, and then **Group Policy Management**.
2) In the console tree, double-click the name of the forest, double-click **Domains**, double-click the name of your domain, double-click **Domain Controllers**, rightclick **Default Domain Controllers Policy**, and then click **Edit**.
3) Under **Computer Configuration**, double-click **Policies**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then click **Audit Policy**.
4) In the details pane, right-click **Audit directory service access**, and then click **Properties**.
5) Select the **Define these policy settings** check box.
6) Under **Audit these attempts**, select the **Success**, check box, and then click **OK**.

Step 2: Set up auditing in object SACLs.

The following procedure presents an example of just one of many different types of SACLs that you can set in AD. You can configure additional SACLs based on the operations that you want to audit.

To set up auditing in object SACLs

1) Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2) Right-click the organizational unit (OU) (or any object) for which you want to enable auditing, and then click **Properties**.
3) Click the **Security** tab, click **Advanced**, and then click the **Auditing** tab.
4) Click **Add**, and under **Enter the object name to select**, type Authenticated Users (or any other security principal), and then click **OK**.
5) In **Apply onto**, click **This object and all descendant objects**.

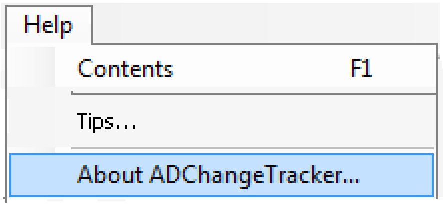
6) Under **Access**, select the **Successful** check box for **Write all properties**. If you want to audit creation and deletion of objects, select the **Successful** check box for **Delete**, **Delete subtree** and **Create all child objects too**.

7) Click **OK** until you exit the property sheet for the OU or other object.

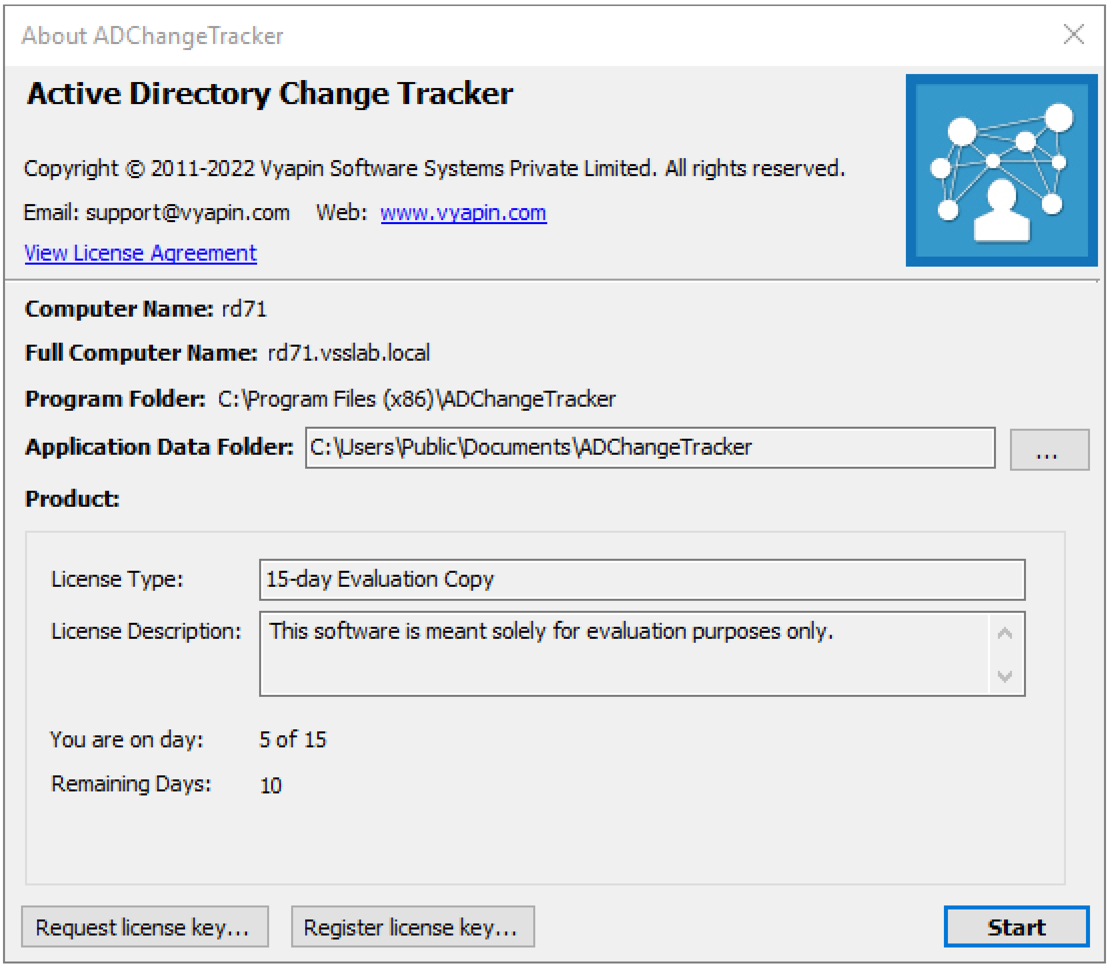
2.2 Change Application Data folder location

ADChangeTracker enables you to change **Application Data** folder location, where its application settings and error log are stored, at any time after installing ADChangeTracker software. To change the Application Data folder location, perform the following steps given below:

1) Select **About ADChangeTracker** from **Help** menu.



2) The **About ADChangeTracker** dialog appears as shown below**:**


About ADChangeTracker

Active Directory Change Tracker

Copyright © 2011-2022 Vyapin Software Systems Private Limited. All rights reserved.

Email: support@vyapin.com Web: www.vyapin.com

View License Agreement

Computer Name: rd71

Full Computer Name: rd71.vsslab.local

Program Folder: C:\Program Files (x86)\ADChangeTracker

Application Data Folder: C:\Users\Public\Documents\ADChangeTracker

Product:

License Type: 15-day Evaluation Copy

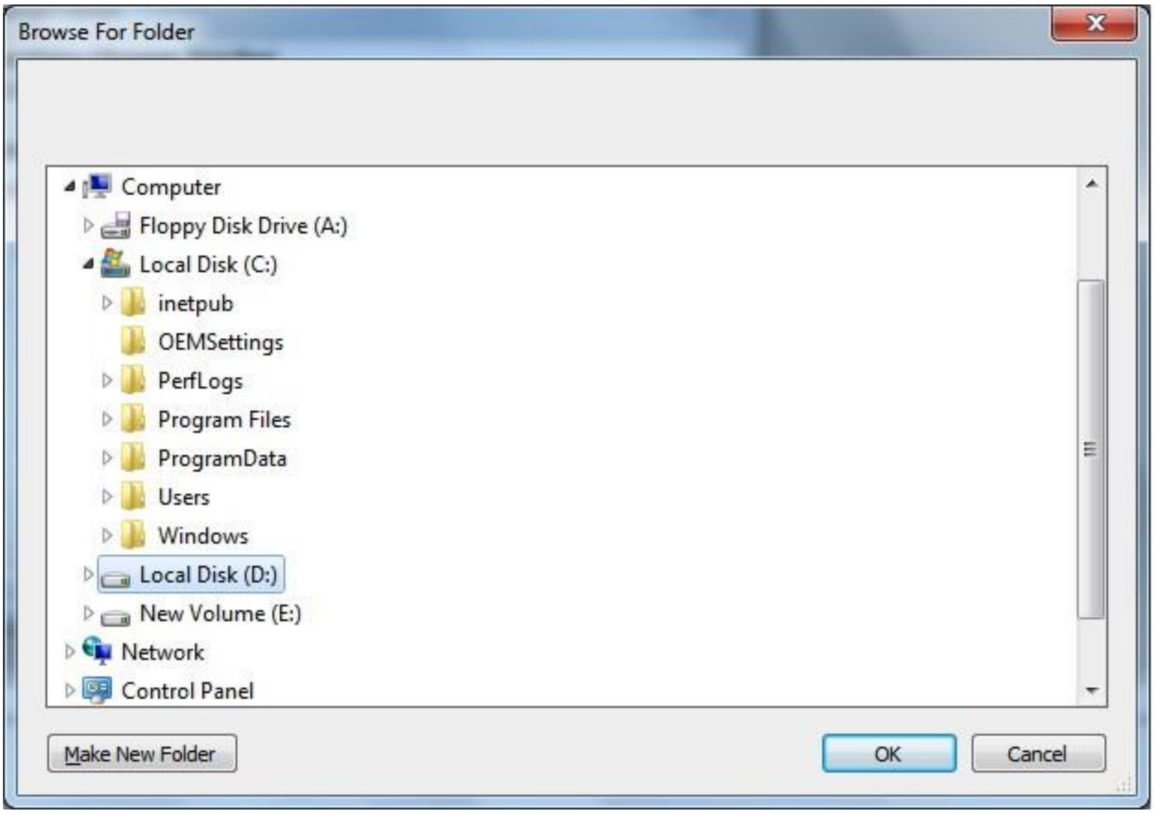
License Description: This software is meant solely for evaluation purposes only.

You are on day: 5 of 15

Remaining Days: 10

3) Click **...** button to change **Application Data** folder location of ADChangeTracker application.

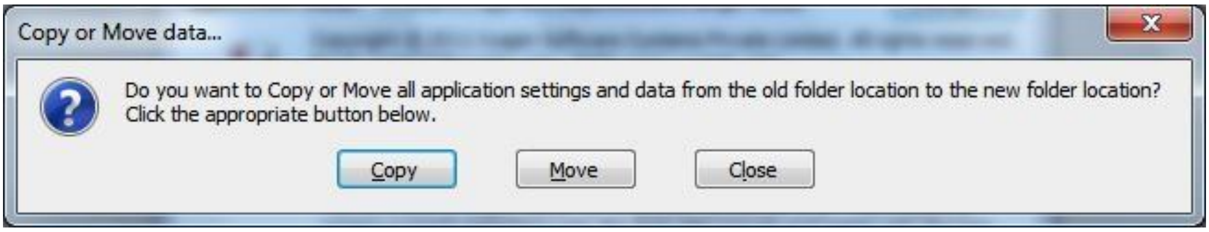
The Browse for Folder location dialog will appear as shown below:



4) Select a desired folder location and Click OK. The folder location can be local drives or mapped network drives.

5) ADChangeTracker provides an option to copy or move the existing

ADChangeTracker application settings and error log to the new location once you change the Application Data Folder. Once you specify the new Application Data folder location, ADChangeTracker will prompt you to copy or move existing ADChangeTracker application settings to the new location as shown below:


Copy or Move data...

Do you want to Copy or Move all application settings and data from the old folder location to the new folder location? Click the appropriate button below.

6) Click the desired action (Copy / Move / Close) to proceed. ADChangeTracker will use the new Application Data folder location henceforth.

2.3 How to Get the Change Made by Value Successfully?

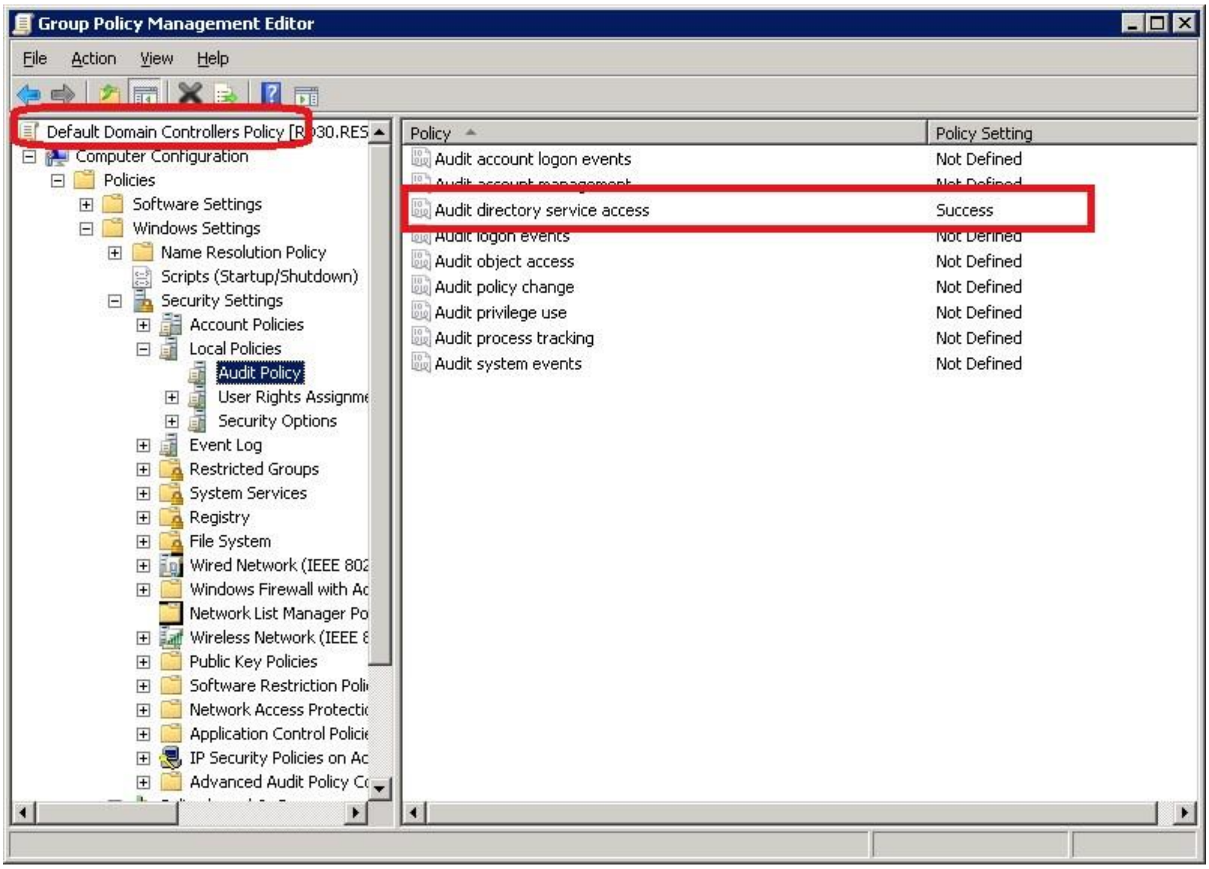
ADChangeTracker reports the 'Change made by' value for all AD objects' changes in the Active Directory. The 'Change made by' is retrieved from the event log of the domain controller in which the change is made. This feature is applicable for **Windows Server 2008 or later** operating systems only.

The 'Change made by' field in the report may sometimes not get reflected immediately after a change is observed in AD (will be empty/blank in the report window). This may be due to a delay/failure in receiving the Event subscription notification by the ADCT Service application. Click Refresh button in the report window to refresh the 'Change made by' field.

If the 'Change made by' value continues to remain unavailable, please ensure the following points in order to retrieve Change made by value successfully:

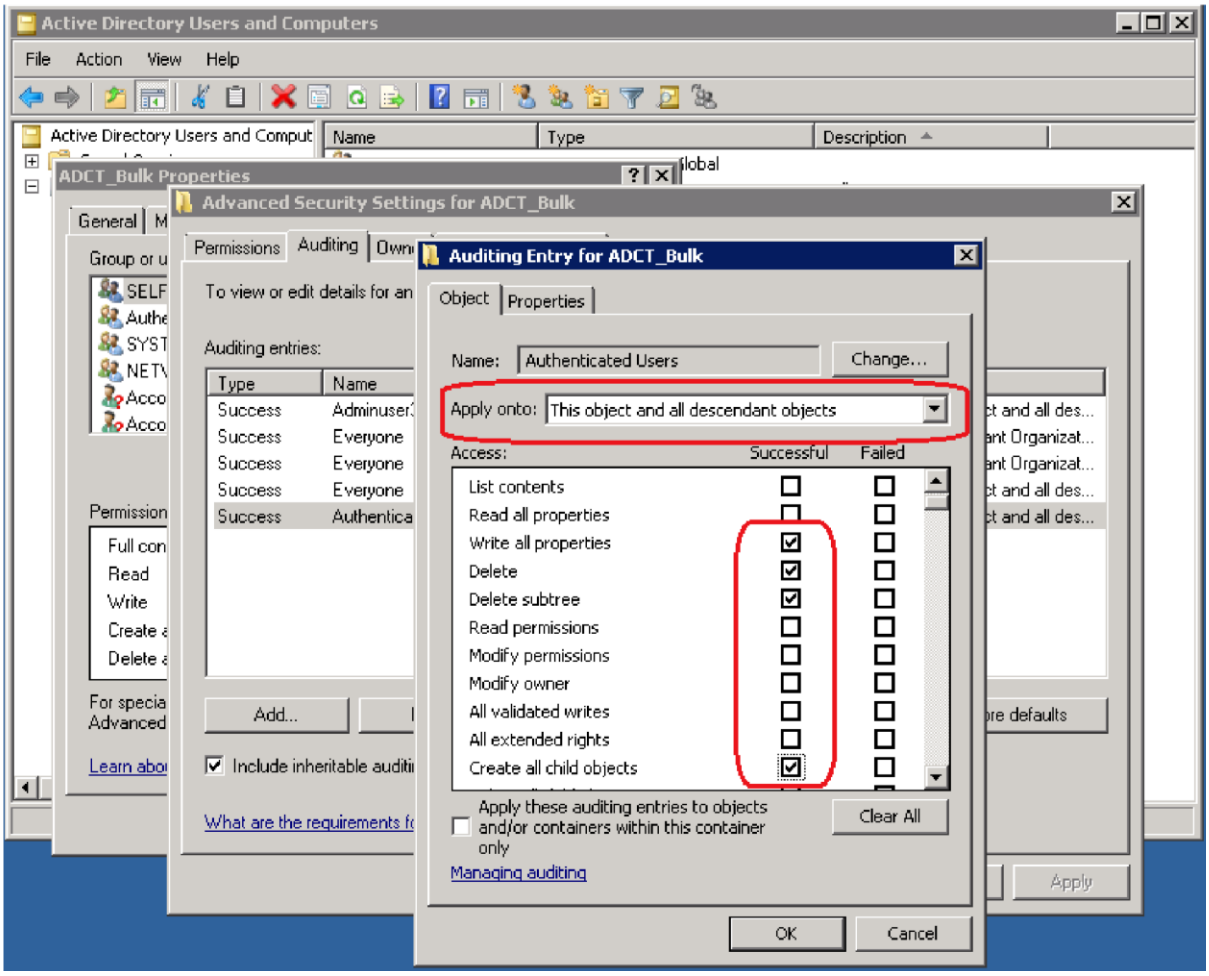
a) Select the 'Use Security event log in DC to retrieve additional Change data (Who & When)' checkbox in the Add domain or Edit domain dialog.

b) Enable the **Audit directory service access** Policy and set to success in **Default Domain Controllers Policy** as shown below:



Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Success
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

c) Select **Write all properties, Delete, Delete subtree** and **Create all child objects** properties for the **OU or domain** in which you wish to track changes as shown below:



Name: Authenticated Users

Apply onto: This object and all descendant objects

Access:	Successful	Failed
List contents	□	□
Read all properties	□	□
Write all properties	☑	□
Delete	☑	□
Delete subtree	☑	□
Read permissions	□	□
Modify permissions	□	□
Modify owner	□	□
All validated writes	□	□
All extended rights	□	□
Create all child objects	☑	□

□ Apply these auditing entries to objects and/or containers within this container only

d) Ensure that there is no Event flooding which may sometimes prevent the ADCT Service application from receiving the subscribed events. For example, ensure that “Read All Properties” is not selected in object’s Auditing. Selecting this setting will create a flurry of events in DC and will cause Event flooding.

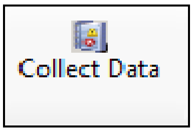
e) Disable firewall protection to read event logs: Ensure that the target Domain Controller is not protected by Windows firewall to read event logs by remote clients.

f) Ensure that the 'ADCT Listener Service' is running in the computer where AD Change Tracker application is installed (can be verified in How to view the subscription status of domain controllers?).

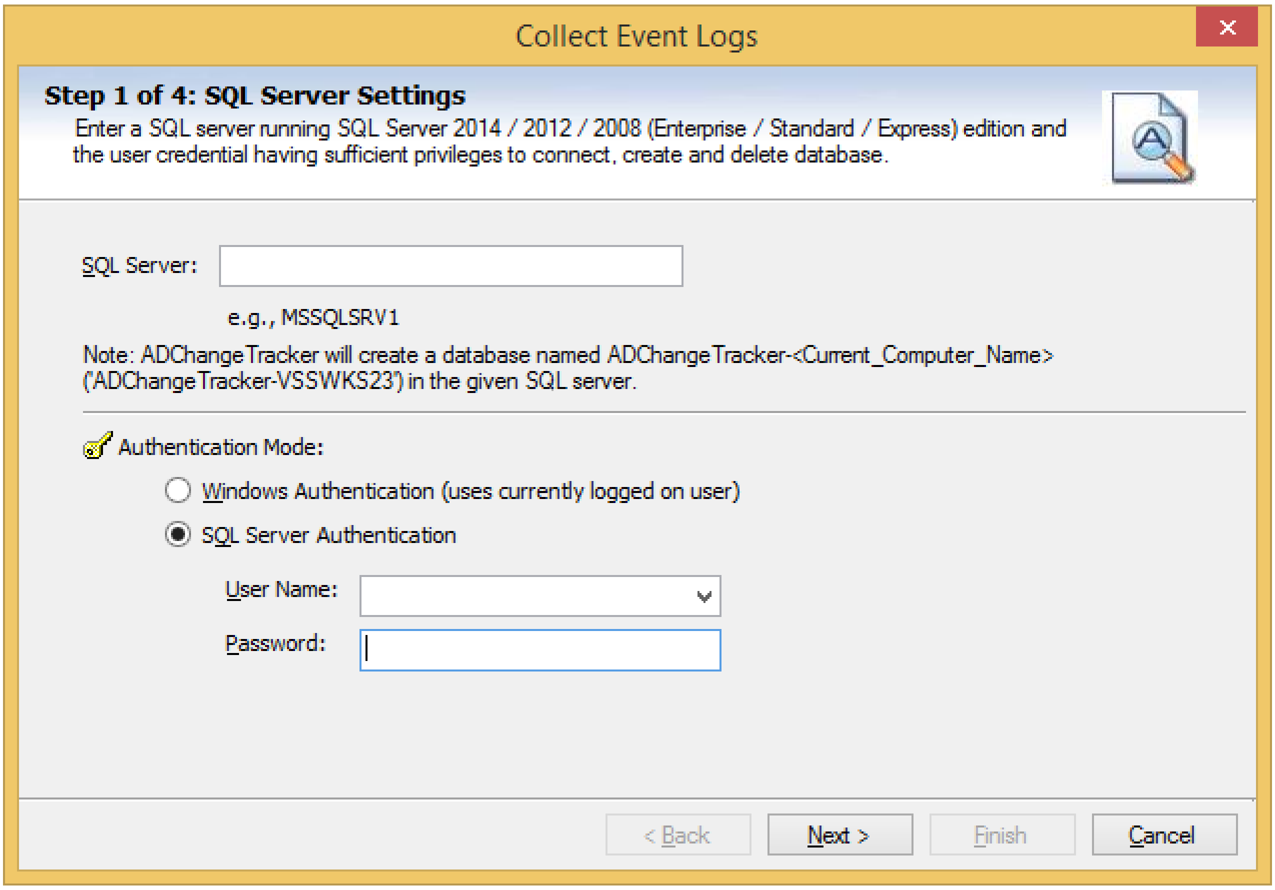
3 ADChangeTracker Features

3.1 Collect Data

The **Collect Data** feature allows you to collect the list of all the events made in Active Directory. You can check for various changes in Active Directory like addition or deletion of objects, modification of properties.

Select 

button in the toolbar. The Collect Event Logs window will be launched..



Collect Event Logs

Step 1 of 4: SQL Server Settings
Enter a SQL server running SQL Server 2014 / 2012 / 2008 (Enterprise / Standard / Express) edition and the user credential having sufficient privileges to connect, create and delete database.

SQL Server:

e.g., MSSQLSRV1

Note: ADChangeTracker will create a database named ADChangeTracker-<Current_Computer_Name> ('ADChangeTracker-VSSWKS23') in the given SQL server.

Authentication Mode:

○ Windows Authentication (uses currently logged on user)

● SQL Server Authentication

User Name:

Password:

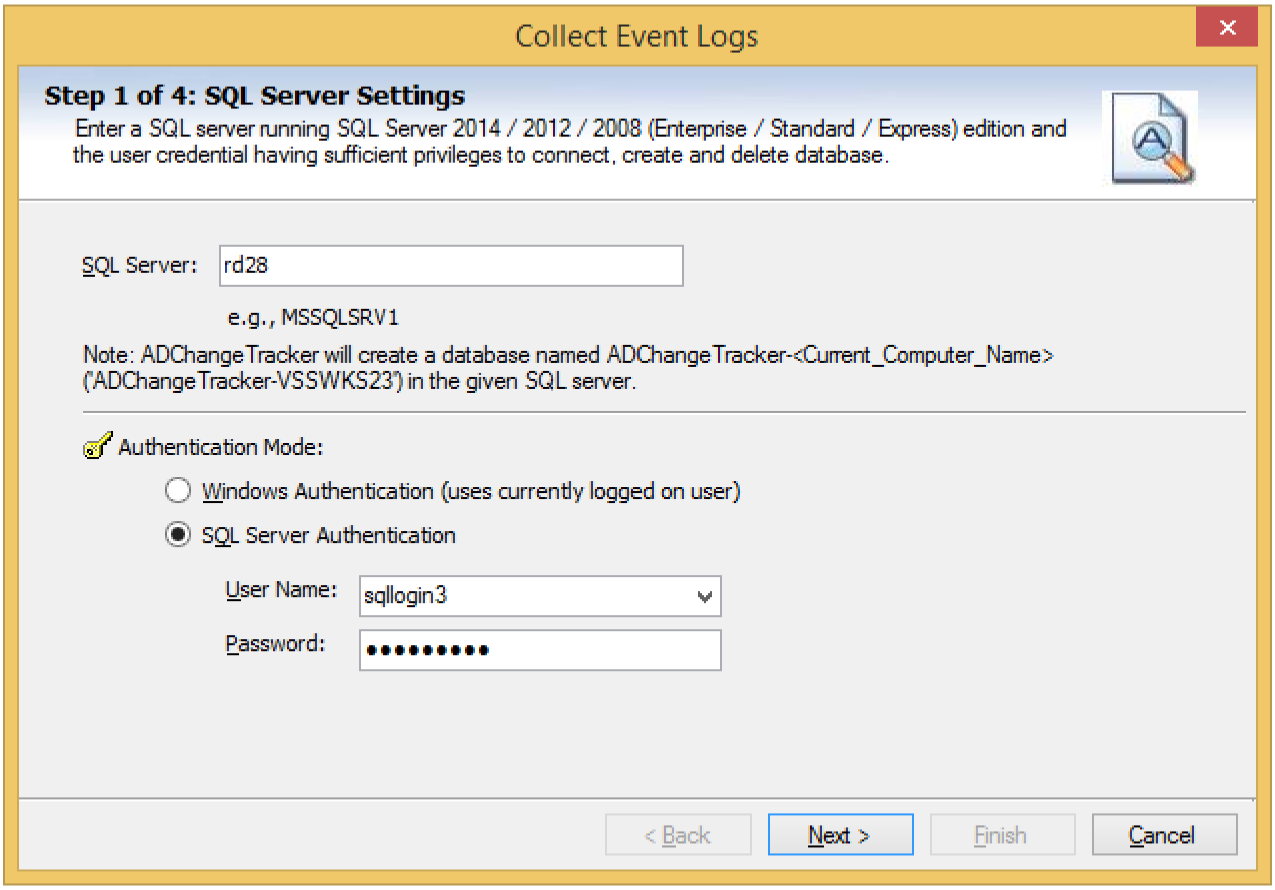
User Authentication

To connect to SQL Server, ADChangeTracker uses the relevant user accounts based on the authentication mode as listed below:

A. **Windows Authentication:**
In this method, ADChangeTracker uses the currently logged on user account while tracking changes using 'Track Now' or the Run as account while using 'Track at scheduled intervals'.

B. **SQL Authentication:**
In this method, ADChangeTracker uses the specified SQL user account and password while tracking changes. ADChangeTracker stores the SQL user name and password as a user profile in 'Stored User Names and Passwords' applet for its usage.

Note: ADChangeTracker expects the user account to have sufficient privileges to create, add to and delete database in the SQL server.



Collect Event Logs

Step 1 of 4: SQL Server Settings

Enter a SQL server running SQL Server 2014 / 2012 / 2008 (Enterprise / Standard / Express) edition and the user credential having sufficient privileges to connect, create and delete database.

SQL Server: rd28

e.g., MSSQLSRV1

Note: ADChangeTracker will create a database named ADChangeTracker-<Current_Computer_Name> ('ADChangeTracker-VSSWKS23') in the given SQL server.

Authentication Mode:

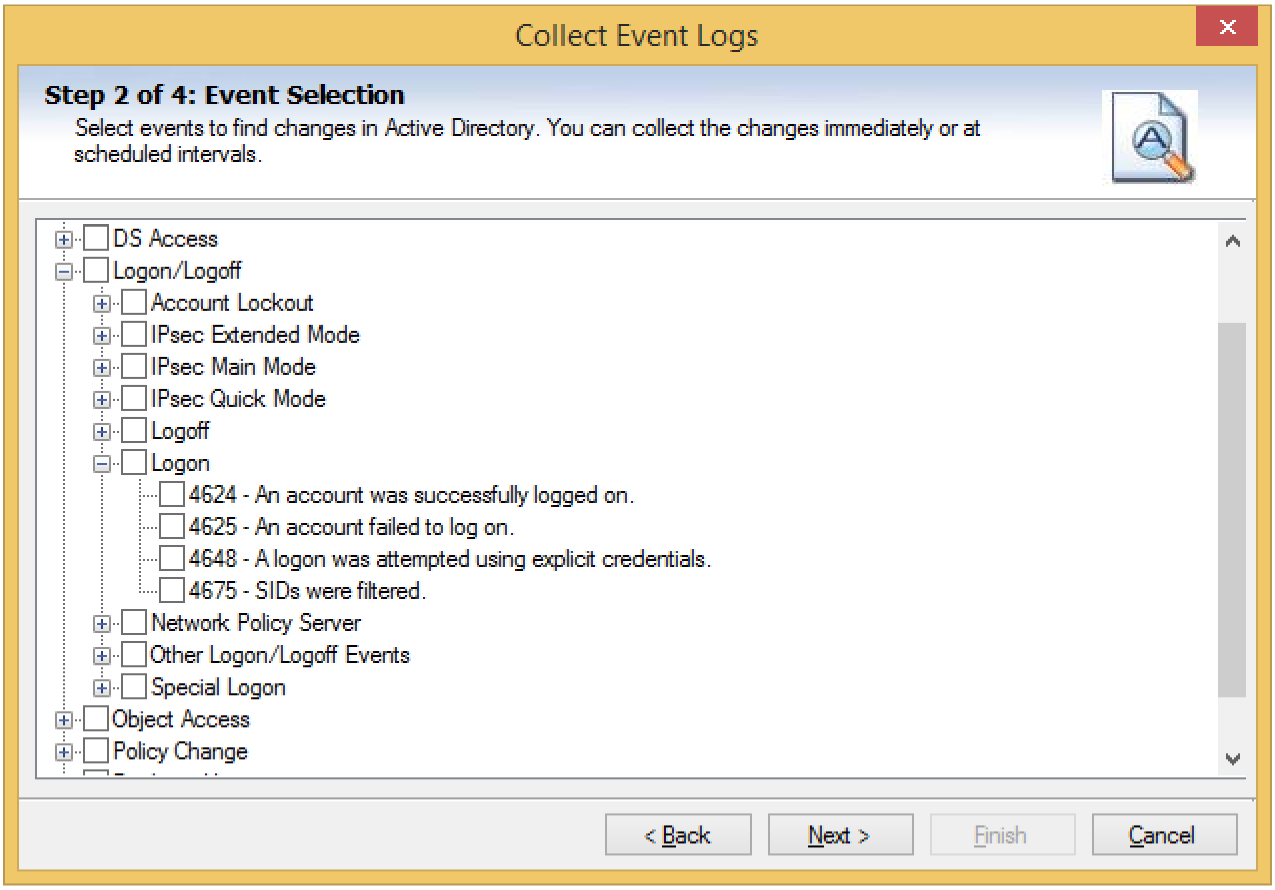
○ Windows Authentication (uses currently logged on user)

● SQL Server Authentication

User Name: sqllogin3

Password: ●●●●●●●●●●

Specify the SQL Server name, authentication mode, user name and password in the above screen and Click **Next** button.



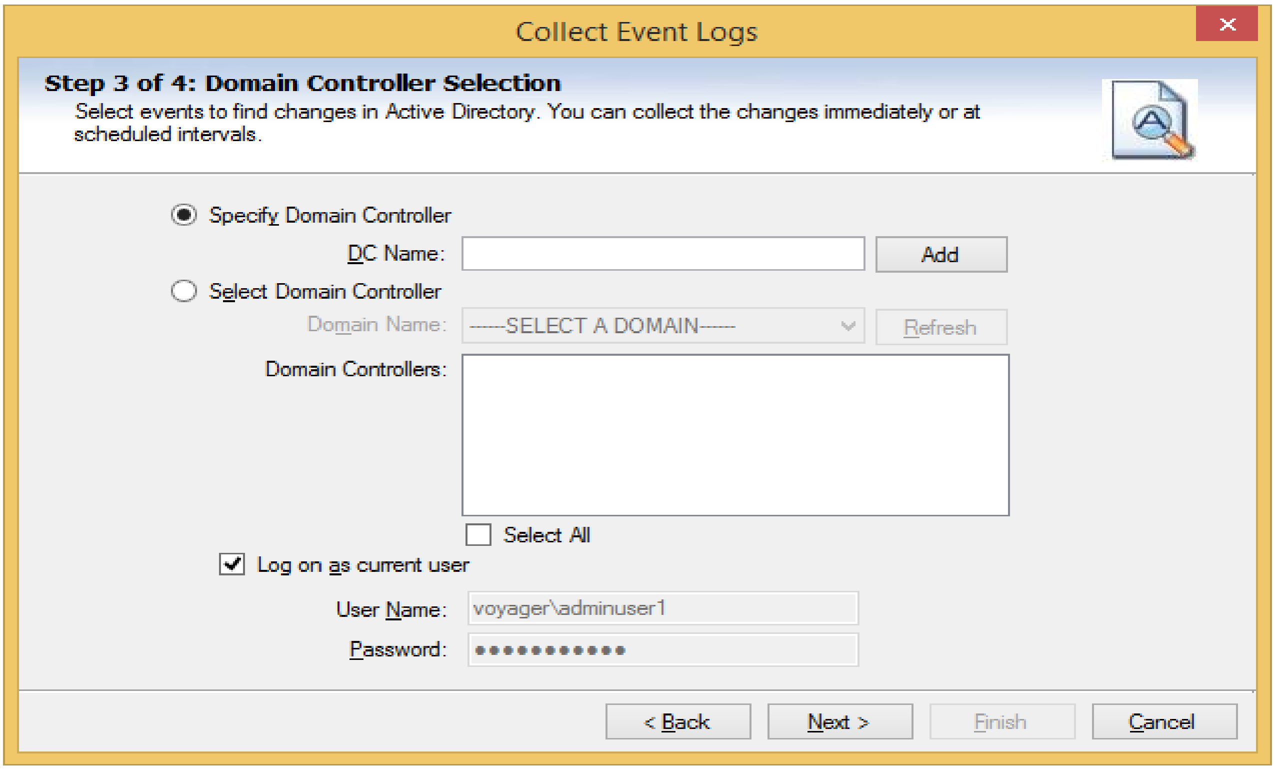
Collect Event Logs

Step 2 of 4: Event Selection

Select events to find changes in Active Directory. You can collect the changes immediately or at scheduled intervals.

- □ DS Access
- □ Logon/Logoff
  - □ Account Lockout
  - □ IPsec Extended Mode
  - □ IPsec Main Mode
  - □ IPsec Quick Mode
  - □ Logoff
  - □ Logon
    - □ 4624 - An account was successfully logged on.
    - □ 4625 - An account failed to log on.
    - □ 4648 - A logon was attempted using explicit credentials.
    - □ 4675 - SIDs were filtered.
  - □ Network Policy Server
  - □ Other Logon/Logoff Events
  - □ Special Logon
- □ Object Access
- □ Policy Change

Select event IDs to find events in Active Directory and Click **Next** button



Collect Event Logs

Step 3 of 4: Domain Controller Selection

Select events to find changes in Active Directory. You can collect the changes immediately or at scheduled intervals.

● Specify Domain Controller

DC Name:

○ Select Domain Controller

Domain Name: ------SELECT A DOMAIN------

Domain Controllers:

□ Select All

☑ Log on as current user

User Name: voyager\adminuser1

Password: ●●●●●●●●●●●●

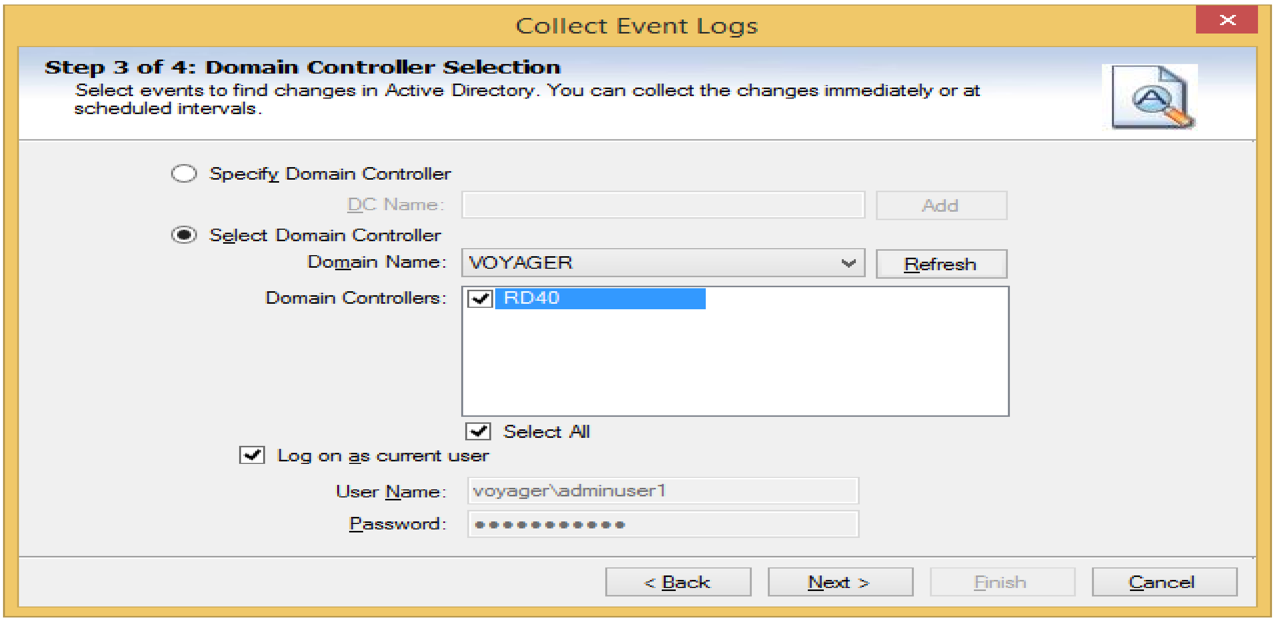
a. In the Specify domain controller, click **Add** button to add a domain to the list using DC Name textbox.

b. The list of domains available in the network will be loaded in the Domain Name dropdown.

c. Select a domain from the Domain Name dropdown.

d. The list of domain controllers for the selected domain will be loaded in the Domain Controller Name dropdown.

Select a domain controller from the Domain Controller Name dropdown.



Collect Event Logs

Step 3 of 4: Domain Controller Selection

Select events to find changes in Active Directory. You can collect the changes immediately or at scheduled intervals.

○ Specify Domain Controller

DC Name:

● Select Domain Controller

Domain Name: VOYAGER

Domain Controllers: ☑ RD40

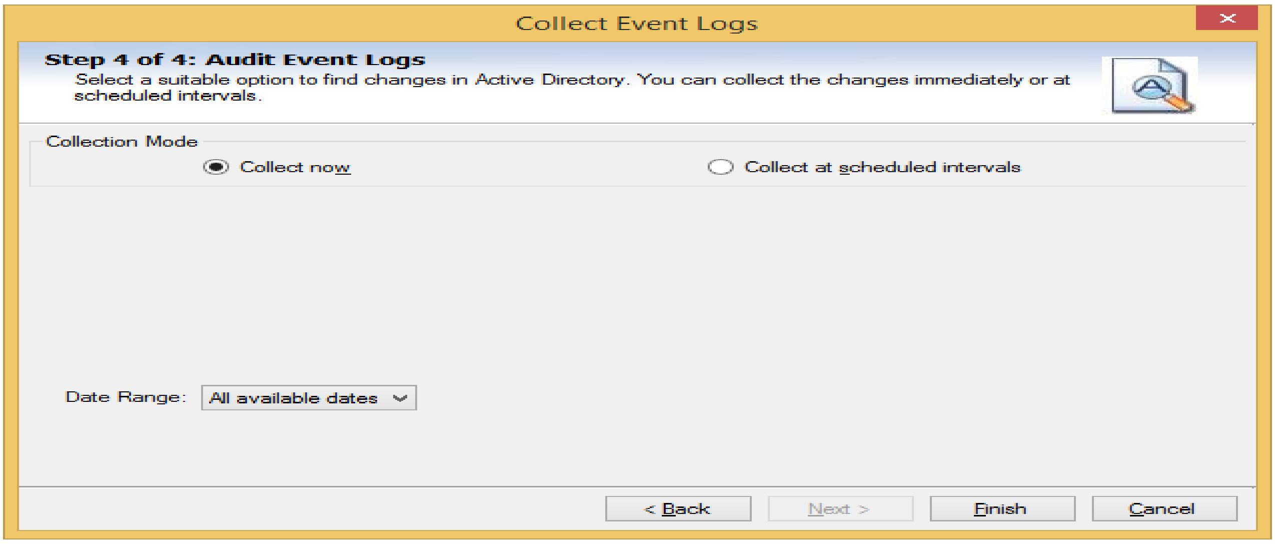
☑ Select All

☑ Log on as current user

User Name: voyager\adminuser1

Password: ●●●●●●●●●●●

Specify user name and the corresponding password to connect to the specified server and Click **Next** button.



Collect Event Logs

Step 4 of 4: Audit Event Logs

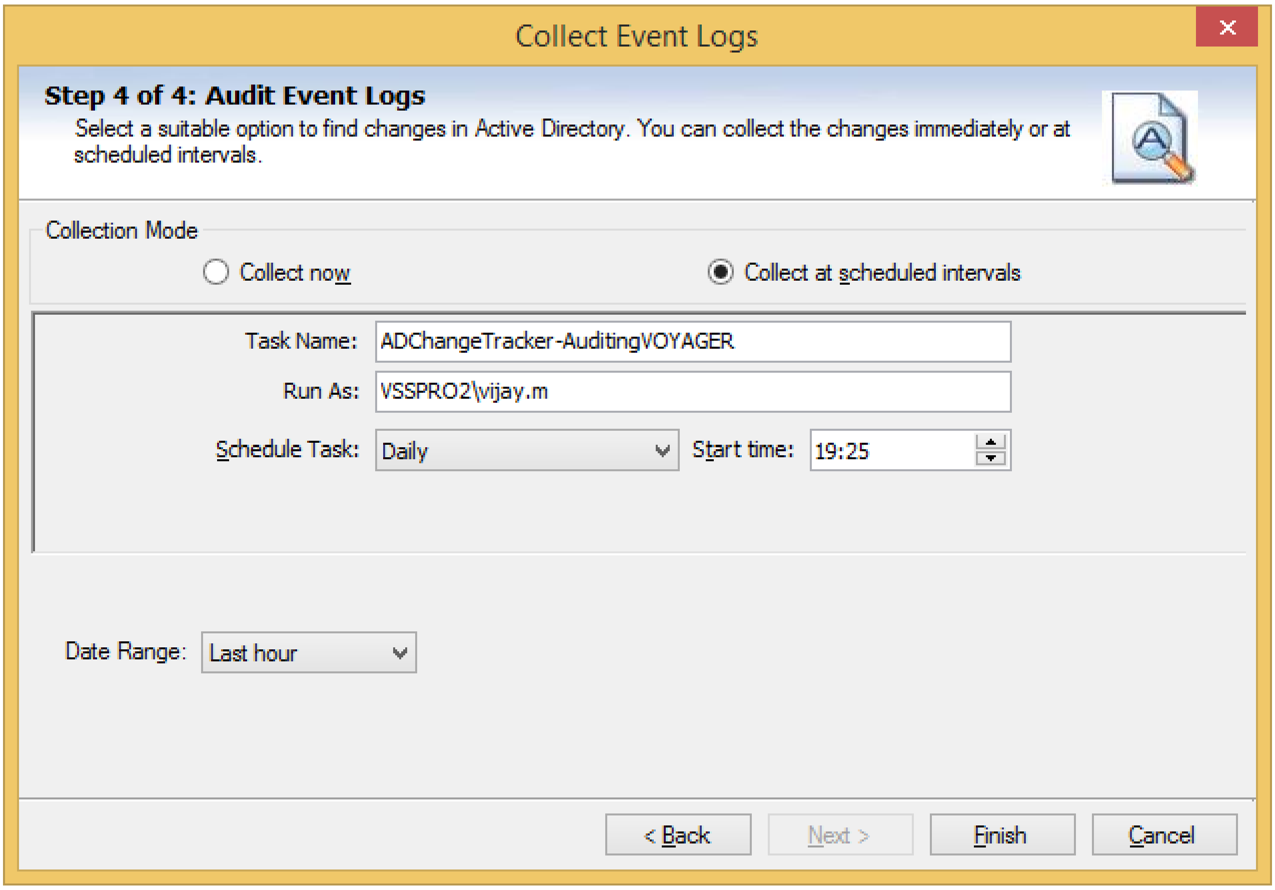
Select a suitable option to find changes in Active Directory. You can collect the changes immediately or at scheduled intervals.

Collection Mode

● Collect now ○ Collect at scheduled intervals

Date Range: All available dates

Select Collect now option to collect events in Active Directory domain immediately upon clicking the Finish button



Step 4 of 4: Audit Event Logs

Select a suitable option to find changes in Active Directory. You can collect the changes immediately or at scheduled intervals.

Collection Mode

○ Collect now ● Collect at scheduled intervals

Task Name: ADChangeTracker-AuditingVOYAGER

Run As: VSSPRO2\vijay.m

Schedule Task: Daily Start time: 19:25

Date Range: Last hour

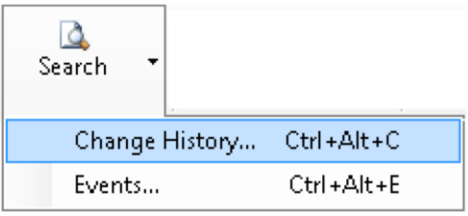
Or select Collect at scheduled intervals option to collect changes made to Active Directory domain at scheduled intervals.

Change the task schedule settings as required and set the password for the specified Run As user and Click **Finish** to save the task details .

Events will be collected since the last time a collect data was performed. The collecting process will only collect the event data and store it in the application's change history database

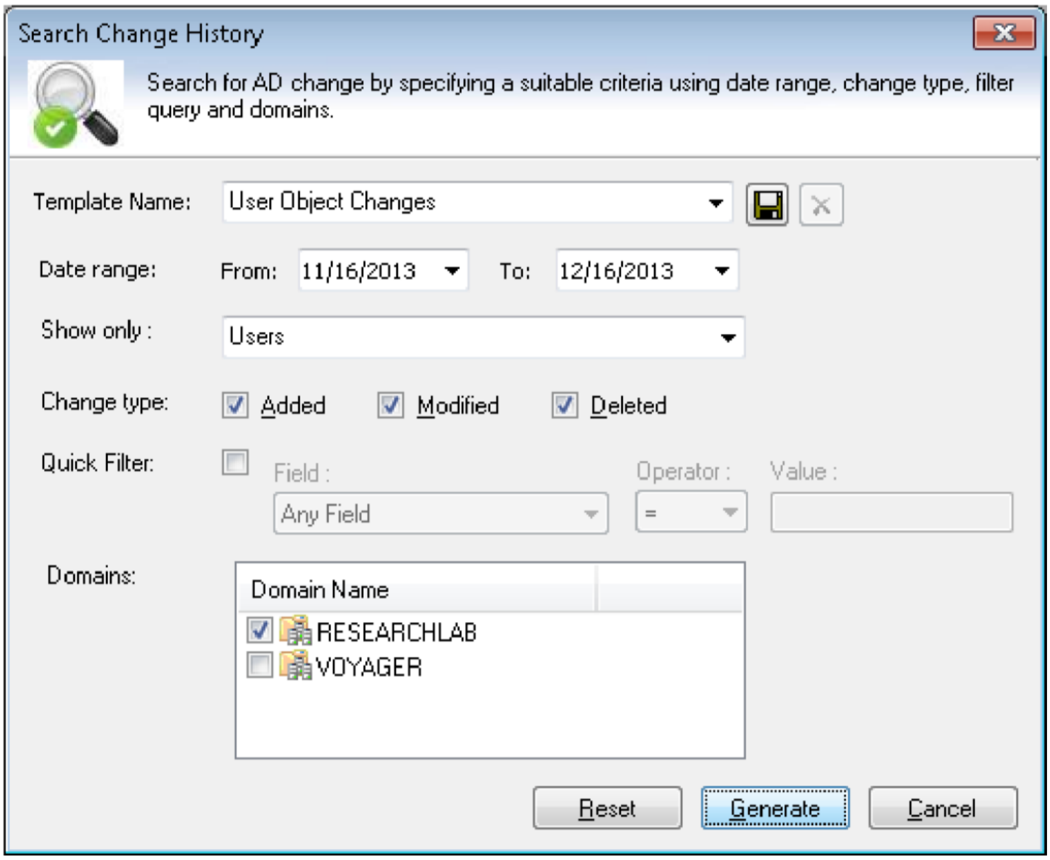
3.2 Search Reports
3.2.1 How to Search Change History?

The **Search Change History** is a powerful feature that allows you to locate specific changes from the past such as 'all newly created user accounts between a time periods'. You can specify a search criteria based on the different search options available.



To launch 'Search Change History' window, click menu in the toolbar. The 'Search Change History' dialog will appear as shown below:

- **Specify** the **Date range, Object type, Change type** and a field based **Filter criteria** to find specific changes in the application's Change History database.
- Select the desired **Domains** to perform your search on.
- Optionally, you can save this search by specifying a name for your search and clicking on the **Save** button. This will save the search for a future use. You can thus maintain a list of your saved searches for repeated use in the future.
- Click on **Generate** button to begin search.



Search Change History

Search for AD change by specifying a suitable criteria using date range, change type, filter query and domains.

Template Name: User Object Changes

Date range: From: 11/16/2013 To: 12/16/2013

Show only : Users

Change type: ☑ Added ☑ Modified ☑ Deleted

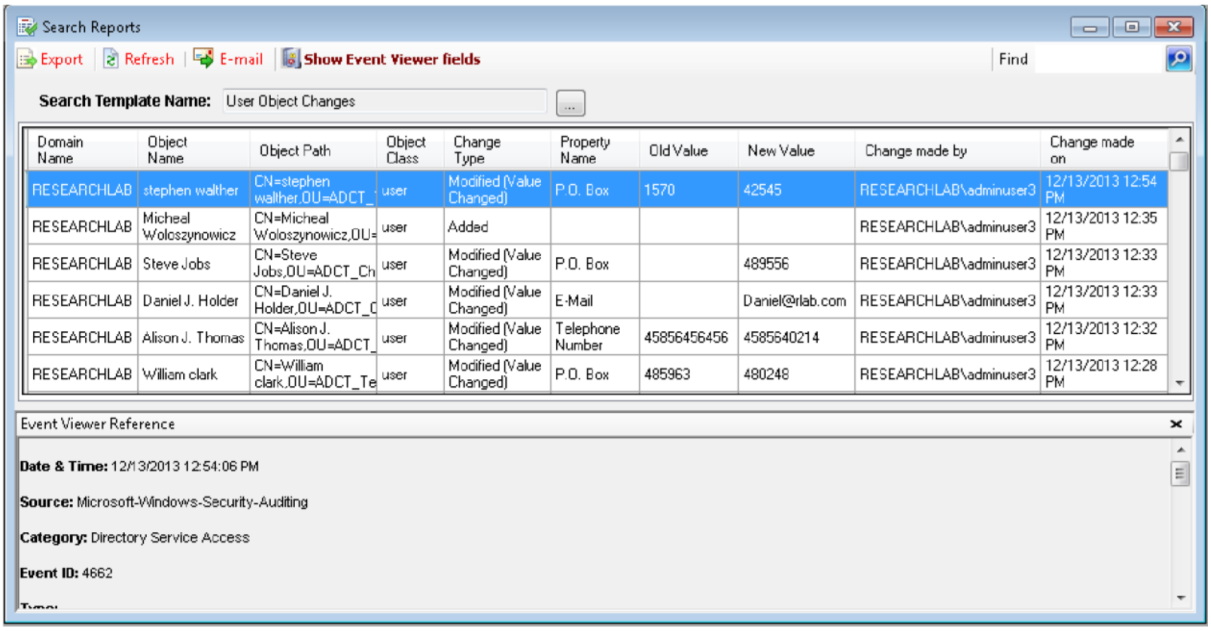
Quick Filter: □ Field : Any Field Operator : = Value :

Domains:

Domain Name
☑ RESEARCHLAB
□ VOYAGER

If you want to use or edit an already saved search, select the name of saved search from the drop down list. This will load the saved search's settings. You may also edit this and click on Save again to save the modified search. Once you load a saved search, you may click Generate to perform a search.

After the data collection process is complete, the report would be generated in a report window as shown below:



Search Template Name: User Object Changes

Domain Name	Object Name	Object Path	Object Class	Change Type	Property Name	Old Value	New Value	Change made by	Change made on
RESEARCHLAB	stephen walther	CN=stephen walther,OU=ADCT_	user	Modified (Value Changed)	P.O. Box	1570	42545	RESEARCHLAB\adminuser3	12/13/2013 12:54 PM
RESEARCHLAB	Micheal Woloszynowicz	CN=Micheal Woloszynowicz,OU=	user	Added				RESEARCHLAB\adminuser3	12/13/2013 12:35 PM
RESEARCHLAB	Steve Jobs	CN=Steve Jobs,OU=ADCT_Ch	user	Modified (Value Changed)	P.O. Box		489556	RESEARCHLAB\adminuser3	12/13/2013 12:33 PM
RESEARCHLAB	Daniel J. Holder	CN=Daniel J. Holder,OU=ADCT_C	user	Modified (Value Changed)	E-Mail		Daniel@rlab.com	RESEARCHLAB\adminuser3	12/13/2013 12:33 PM
RESEARCHLAB	Alison J. Thomas	CN=Alison J. Thomas,OU=ADCT_	user	Modified (Value Changed)	Telephone Number	45856456456	4585640214	RESEARCHLAB\adminuser3	12/13/2013 12:32 PM
RESEARCHLAB	William clark	CN=William clark,OU=ADCT_Te	user	Modified (Value Changed)	P.O. Box	485963	480248	RESEARCHLAB\adminuser3	12/13/2013 12:28 PM

Event Viewer Reference

Date & Time: 12/13/2013 12:54:06 PM

Source: Microsoft-Windows-Security-Auditing

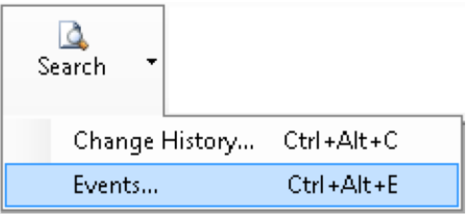
Category: Directory Service Access

Event ID: 4662

Type:

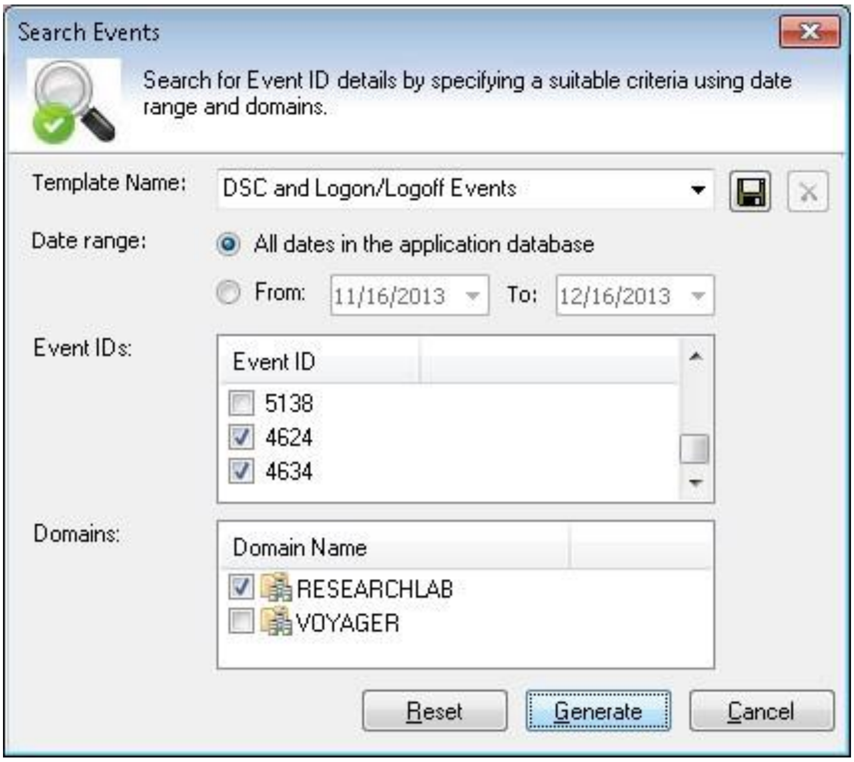
3.2.2 How to Search Events?

The **Search Events** is a powerful feature that allows you to locate specific events that occurred over a time period and stored in the application's Events History database.



To launch 'Search Events' window, click menu in the toolbar. The 'Search Events' dialog will appear as shown below:

- ➢ Specify the **Date range** and **Event IDs** to find in the application’s Events History database. You can also select multiple events for search.
- ➢ You can also perform the events search for the entire database by selecting the **All dates in the application database** option.
- ➢ Select the desired **Domains** to perform your search on.
- ➢ Optionally, you can save this search by specifying a name for your search and clicking on the Save button. This will save the search for a future use. You can thus maintain a list of your saved searches for repeated use in the future.
- ➢ Click **Generate** button to begin search.



Search Events

Search for Event ID details by specifying a suitable criteria using date range and domains.

Template Name: DSC and Logon/Logoff Events

Date range: ● All dates in the application database

○ From: 11/16/2013 To: 12/16/2013

Event IDs:

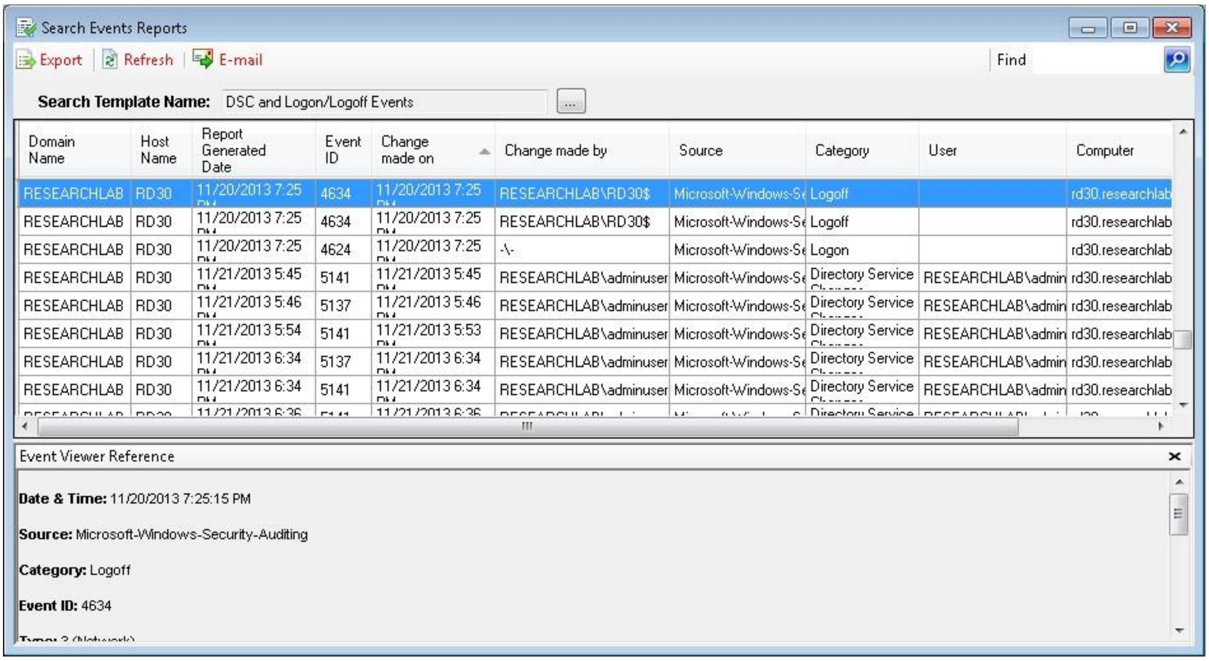
Event ID
□ 5138
☑ 4624
☑ 4634

Domains:

Domain Name
☑ RESEARCHLAB
□ VOYAGER

If you want to use an already saved search, select the name of saved search from the drop down list. This will load the saved search's settings. Once you load a saved search, you may click **Generate** to perform a search.

After the data collection process is complete, the report would be generated in a report window as shown below:



Search Template Name: DSC and Logon/Logoff Events

Domain Name	Host Name	Report Generated Date	Event ID	Change made on	Change made by	Source	Category	User	Computer
RESEARCHLAB	RD30	11/20/2013 7:25	4634	11/20/2013 7:25	RESEARCHLAB\RD30$	Microsoft-Windows-Se	Logoff		rd30.researchlab
RESEARCHLAB	RD30	11/20/2013 7:25	4634	11/20/2013 7:25	RESEARCHLAB\RD30$	Microsoft-Windows-Se	Logoff		rd30.researchlab
RESEARCHLAB	RD30	11/20/2013 7:25	4624	11/20/2013 7:25	-\-	Microsoft-Windows-Se	Logon		rd30.researchlab
RESEARCHLAB	RD30	11/21/2013 5:45	5141	11/21/2013 5:45	RESEARCHLAB\adminuser	Microsoft-Windows-Se	Directory Service	RESEARCHLAB\admin	rd30.researchlab
RESEARCHLAB	RD30	11/21/2013 5:46	5137	11/21/2013 5:46	RESEARCHLAB\adminuser	Microsoft-Windows-Se	Directory Service	RESEARCHLAB\admin	rd30.researchlab
RESEARCHLAB	RD30	11/21/2013 5:54	5141	11/21/2013 5:53	RESEARCHLAB\adminuser	Microsoft-Windows-Se	Directory Service	RESEARCHLAB\admin	rd30.researchlab
RESEARCHLAB	RD30	11/21/2013 6:34	5137	11/21/2013 6:34	RESEARCHLAB\adminuser	Microsoft-Windows-Se	Directory Service	RESEARCHLAB\admin	rd30.researchlab
RESEARCHLAB	RD30	11/21/2013 6:34	5141	11/21/2013 6:34	RESEARCHLAB\adminuser	Microsoft-Windows-Se	Directory Service	RESEARCHLAB\admin	rd30.researchlab

Event Viewer Reference

Date & Time: 11/20/2013 7:25:15 PM

Source: Microsoft-Windows-Security-Auditing

Category: Logoff

Event ID: 4634

Type: 3 (Network)

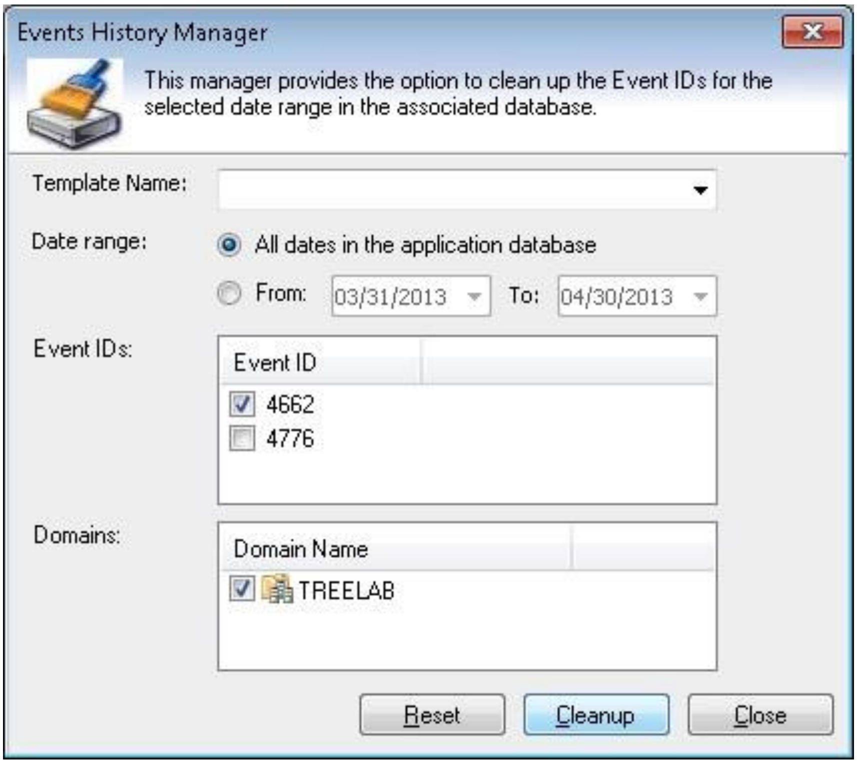
3.3 History Manager

3.3.1 How to Cleanup Events History?

The Events History Manager allows you to clean up any unwanted events and their related data from the Events History database. The Events History database contains all events from the time you configured the specified event ID in the application. Please be careful while you perform cleanups of events as this will permanently delete the selected events from your database. It is highly recommended that you maintain a full backup of the application’s database at regular intervals to recover any accidental loss of events data.

To launch 'Events History Manager' window, click History Manager menu in the toolbar. The 'Events History Manager' dialog will appear as shown below:

- Specify the **Date range** and **Event IDs** to cleanup specific event ID in the application’s Events History database.
- Select the desired **Domains** to perform the cleanup.
- Optionally, you can cleanup the events by selecting a template from the saved templates.
- Click on **Cleanup** button to delete all the events for the selected date range and domain.



Events History Manager

This manager provides the option to clean up the Event IDs for the selected date range in the associated database.

Template Name:

Date range: ● All dates in the application database

○ From: 03/31/2013 To: 04/30/2013

Event IDs:

Event ID
☑ 4662
□ 4776

Domains:

Domain Name
☑ TREELAB

NOTE: You can also delete the entire events history by selecting the 'All dates in the application database' option.

3.4 Events Reports

3.4.1 About Events Reports

Events Reports in ADChangeTracker is a powerful feature that enables the user to report the events data for **AD object changes, User logon/logoff activities, Password change activities and Terminal Services activities** based on specific event ID(s) in the security event log of domain controller. This feature is powered by a listener Service called **ADCT Listener Service**. ADCT Listener Service collects the events data and stores in the application's Events History database. You can view events data by specifying the timestamp, domain, change type, category and field based filter query that occurred over a time period.

Benefits

- Reports User Logon/Logoff activities in a domain with valuable information like Client Name, Logon Type and Workstation Name.
- Reports events data with When and Who made the changes for Password change activities in Active Directory.
- Reports Terminal Services Activities of roaming users in a domain with valuable information like Connected User Name, Workstation Name and Session Type.
- Reports What exactly changed, along with Old Value and New Value, When the change was made, Where the change was made in Active Directory and Who made the changes in Active Directory objects.

3.4.2 Configure Events Reports

This section provides step-by-step procedure for configuring Events Reports. This process consists of three primary steps:

- Enable audit policy.
- Configure event ID(s) in application for security event log data collection.
- Set up auditing in object's SACL. This step is applicable for Object Change Reports and Permissions Change Reports only.

Enable audit policy

1. Click **Start**, point to **Administrative Tools**, and then **Group Policy Management**.
2. In the console tree, double-click the name of the forest, double-click **Domains**, double-click the name of your domain, double-click **Domain Controllers**, rightclick **Default Domain Controllers Policy**, and then click **Edit**.
3. Under **Computer Configuration**, double-click **Policies**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then click **Audit Policy**.
4. In the details pane, right-click the Policy pertaining to the report as shown in the following table and then click **Properties**.

Report Name	Policy
User Logon/Logoff Reports	Audit logon events
Password Change Reports	Audit account management
Terminal Services Activity Reports	Audit logon events
Object Change Reports	Audit directory service access
Permissions Change Reports	Audit directory service access

5. Select the **Define these policy settings** check box.
6. Under **Audit these attempts**, select the **Success** check box, and then click OK.

Configure event ID(s) in application for security event log data collection.

For security event log data collection, configure event ID(s) corresponding to each report in **Real Time Events** -> **Alerts** as stated in the following table:

Report Name	Event ID(s)
User Logon/Logoff Reports	**4624, 4634**

Password Change Reports	**4724**
Terminal Services Activity Reports	**4778, 4779**
Object Change Reports	**5136, 5137, 5139, 5141**
Permissions Change Reports	**5136**

Set up auditing in object's SACL:

To set up **SACL** auditing for directory objects, perform the following steps.

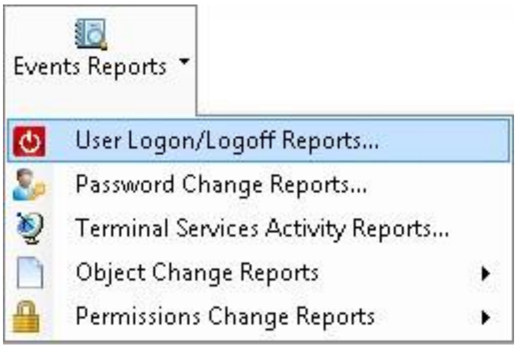
1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Right-click the organizational unit or any object for which you want to enable auditing, and then click **Properties**.
3. Click the **Security** tab, click **Advanced**, and then click the **Auditing** tab.
4. Click **Add**, and under **Enter the object name to select**, type Authenticated Users (or any other security principal), and then click **OK**.
5. In **Apply onto**, click **This object and all descendant objects**.
6. For **Object Change Reports**: Under **Access**, select the **Successful** check box for **Write all properties**. If you want to report events data for creation and deletion of objects, select the **Successful** check box for **Delete, Delete subtree** and **Create all child objects too**.
7. For **Permission Change Reports**: Under **Access**, select the **Successful** check box for **Modify Permissions**.
8. Click **OK** until you exit the property sheet of the organizational unit or other object.

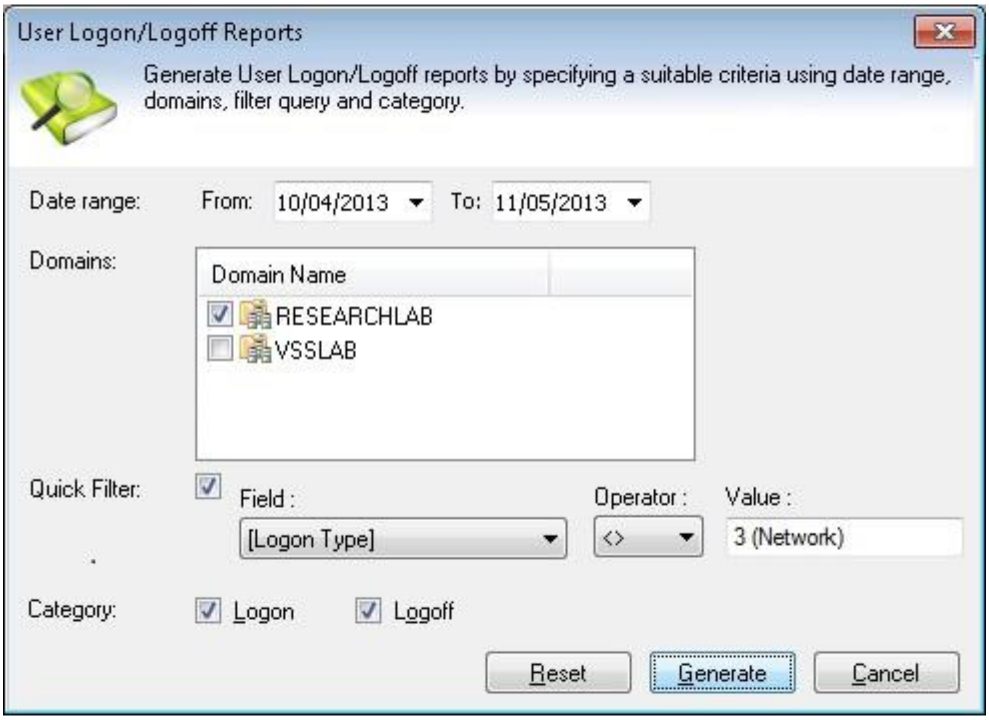
3.4.3 How to generate User Logon/Logoff Reports?

To generate the User Logon/Logoff Reports, perform the following steps.

1. Configure settings for 'User Logon/Logoff Reports' as stated in Configure Events Reports.

2. To launch 'User Logon/Logoff Reports' window, click menu in the toolbar. The 'User Logon/Logoff Reports' window will appear as shown below:


Events Reports
User Logon/Logoff Reports...
Password Change Reports...
Terminal Services Activity Reports...
Object Change Reports
Permissions Change Reports



Generate User Logon/Logoff reports by specifying a suitable criteria using date range, domains, filter query and category.

Date range: From: 10/04/2013 To: 11/05/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

Quick Filter: ☑ Field : [Logon Type] Operator : <> Value : 3 (Network)

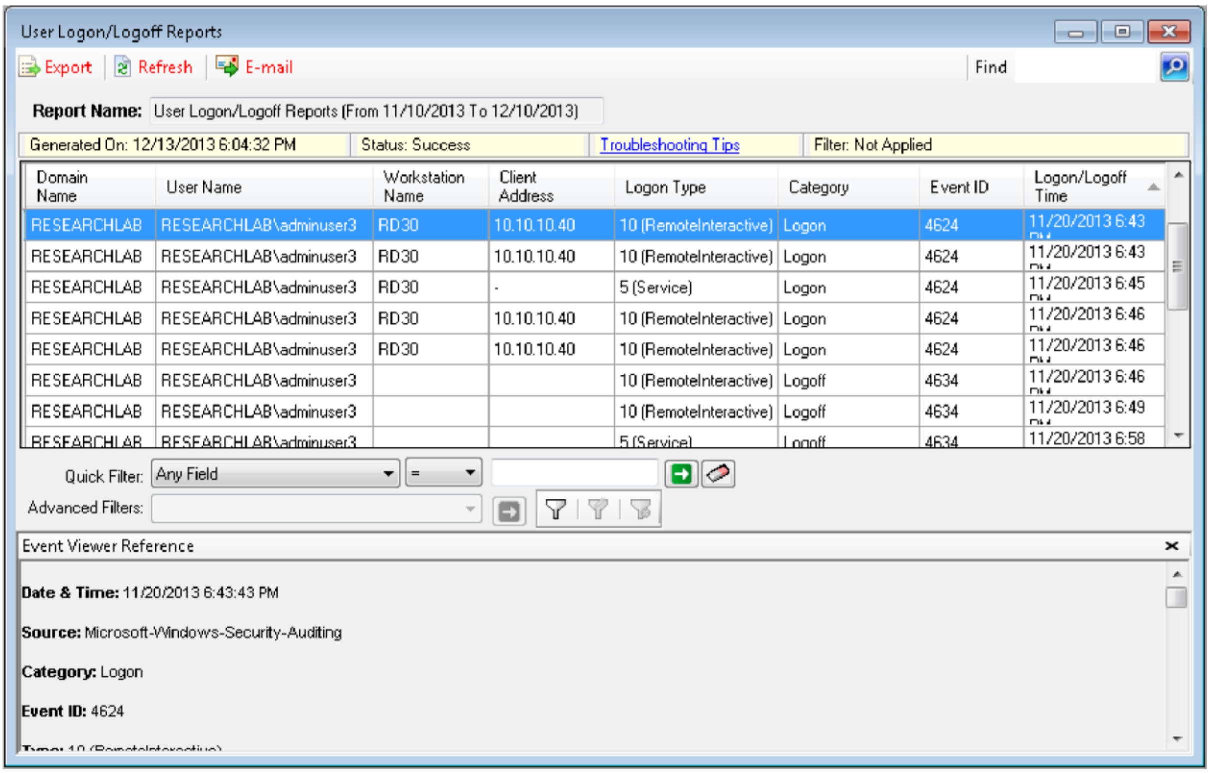
Category: ☑ Logon ☑ Logoff

3. Specify the Date range, Category and a field based Filter criteria to find the User logon/logoff events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: User Logon/Logoff Reports (From 11/10/2013 To 12/10/2013)

Generated On: 12/13/2013 6:04:32 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	User Name	Workstation Name	Client Address	Logon Type	Category	Event ID	Logon/Logoff Time
RESEARCHLAB	RESEARCHLAB\adminuser3	RD30	10.10.10.40	10 (RemoteInteractive)	Logon	4624	11/20/2013 6:43 PM
RESEARCHLAB	RESEARCHLAB\adminuser3	RD30	10.10.10.40	10 (RemoteInteractive)	Logon	4624	11/20/2013 6:43 PM
RESEARCHLAB	RESEARCHLAB\adminuser3	RD30	-	5 (Service)	Logon	4624	11/20/2013 6:45 PM
RESEARCHLAB	RESEARCHLAB\adminuser3	RD30	10.10.10.40	10 (RemoteInteractive)	Logon	4624	11/20/2013 6:46 PM
RESEARCHLAB	RESEARCHLAB\adminuser3	RD30	10.10.10.40	10 (RemoteInteractive)	Logon	4624	11/20/2013 6:46 PM
RESEARCHLAB	RESEARCHLAB\adminuser3			10 (RemoteInteractive)	Logoff	4634	11/20/2013 6:46 PM
RESEARCHLAB	RESEARCHLAB\adminuser3			10 (RemoteInteractive)	Logoff	4634	11/20/2013 6:49 PM
RESEARCHLAB	RESEARCHLAB\adminuser3			5 (Service)	Logoff	4634	11/20/2013 6:58

Quick Filter: Any Field =

Advanced Filters:

Event Viewer Reference

Date & Time: 11/20/2013 6:43:43 PM

Source: Microsoft-Windows-Security-Auditing

Category: Logon

Event ID: 4624

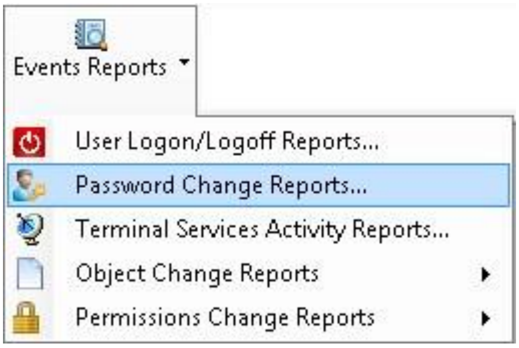
Type: 10 (RemoteInteractive)

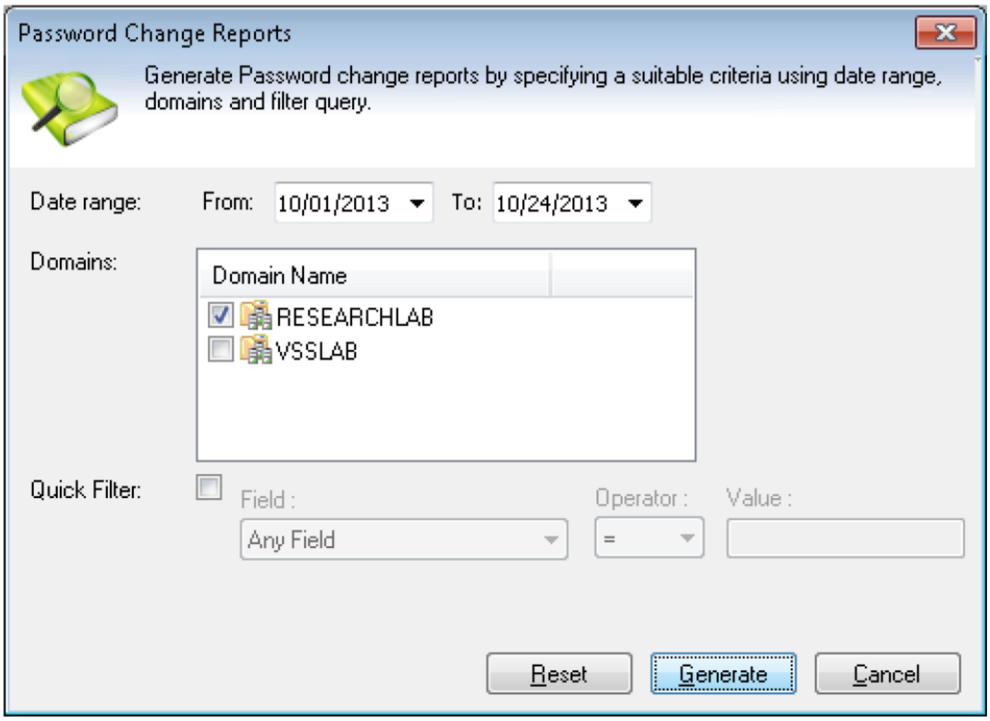
3.4.4 How to generate Password Change Reports?

To generate the Password Change Reports, perform the following steps.

1. Configure settings for 'Password Change Reports' as stated in Configure Events Reports.

2. To launch 'Password Change Reports' window, click menu in the toolbar. The 'Password Change Reports' window will appear as shown below:


Events Reports
User Logon/Logoff Reports...
Password Change Reports...
Terminal Services Activity Reports...
Object Change Reports
Permissions Change Reports



Password Change Reports

Generate Password change reports by specifying a suitable criteria using date range, domains and filter query.

Date range: From: 10/01/2013 To: 10/24/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

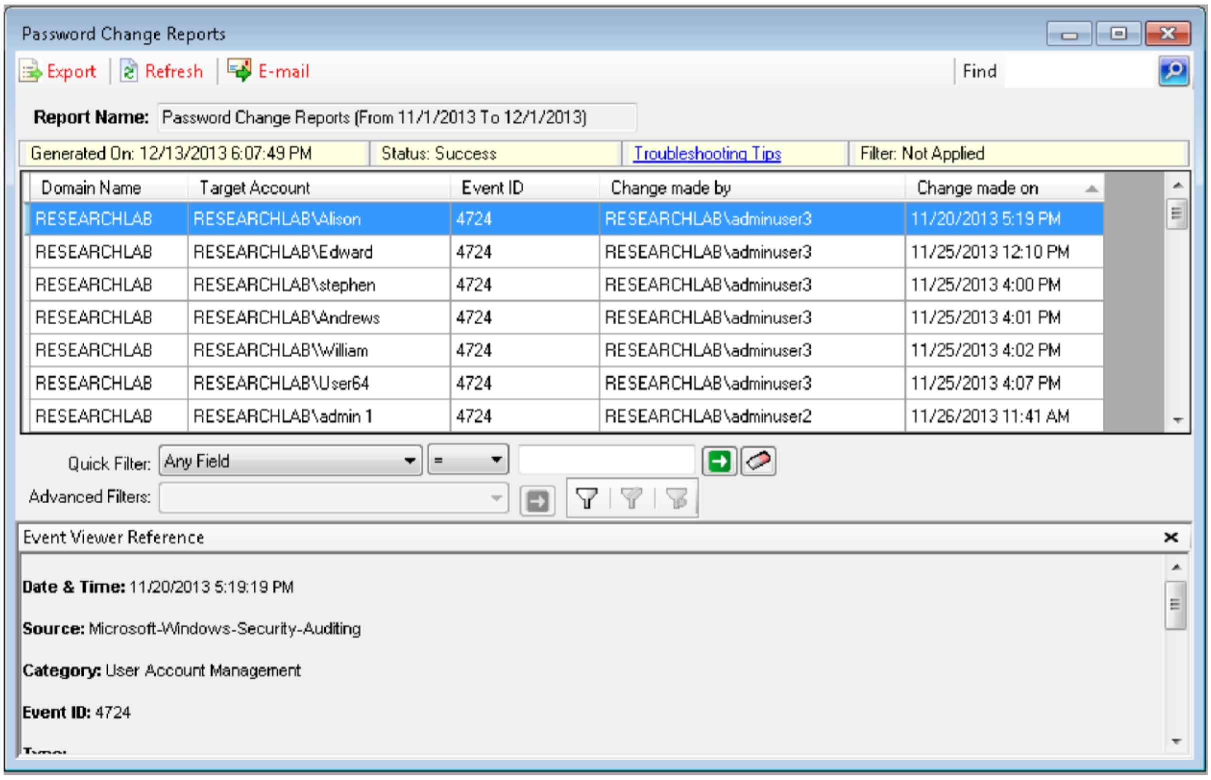
Quick Filter: □ Field : Any Field Operator : = Value :

3. Specify the Date range and a field based Filter criteria to find the Password change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Password Change Reports (From 11/1/2013 To 12/1/2013)

Generated On: 12/13/2013 6:07:49 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Target Account	Event ID	Change made by	Change made on
RESEARCHLAB	RESEARCHLAB\Alison	4724	RESEARCHLAB\adminuser3	11/20/2013 5:19 PM
RESEARCHLAB	RESEARCHLAB\Edward	4724	RESEARCHLAB\adminuser3	11/25/2013 12:10 PM
RESEARCHLAB	RESEARCHLAB\stephen	4724	RESEARCHLAB\adminuser3	11/25/2013 4:00 PM
RESEARCHLAB	RESEARCHLAB\Andrews	4724	RESEARCHLAB\adminuser3	11/25/2013 4:01 PM
RESEARCHLAB	RESEARCHLAB\William	4724	RESEARCHLAB\adminuser3	11/25/2013 4:02 PM
RESEARCHLAB	RESEARCHLAB\User64	4724	RESEARCHLAB\adminuser3	11/25/2013 4:07 PM
RESEARCHLAB	RESEARCHLAB\admin 1	4724	RESEARCHLAB\adminuser2	11/26/2013 11:41 AM

Quick Filter: Any Field =

Advanced Filters:

Event Viewer Reference

Date & Time: 11/20/2013 5:19:19 PM

Source: Microsoft-Windows-Security-Auditing

Category: User Account Management

Event ID: 4724

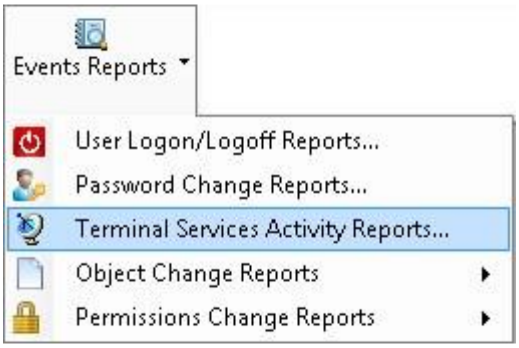
Type:

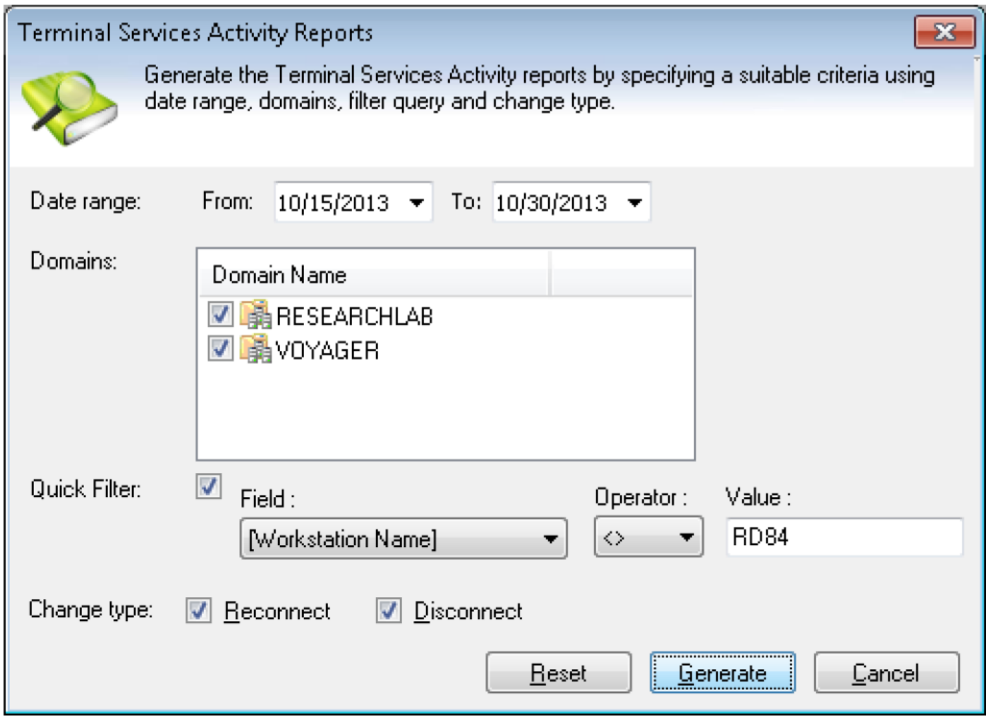
3.4.5 How to generate Terminal Services Activity Reports?

To generate the **Terminal Services Activity Reports,** perform the following steps.

1. Configure settings for 'Terminal Services Activity Reports' as stated in Configure Events Reports.

2. To launch 'Terminal Services Activity Reports' window, click menu in the toolbar. The 'Terminal Services Activity Reports' window will appear as shown below:


Events Reports
User Logon/Logoff Reports...
Password Change Reports...
Terminal Services Activity Reports...
Object Change Reports
Permissions Change Reports



Generate the Terminal Services Activity reports by specifying a suitable criteria using date range, domains, filter query and change type.

Date range: From: 10/15/2013 To: 10/30/2013

Domains:

Domain Name
☑ RESEARCHLAB
☑ VOYAGER

Quick Filter: ☑ Field : [Workstation Name] Operator : <> Value : RD84

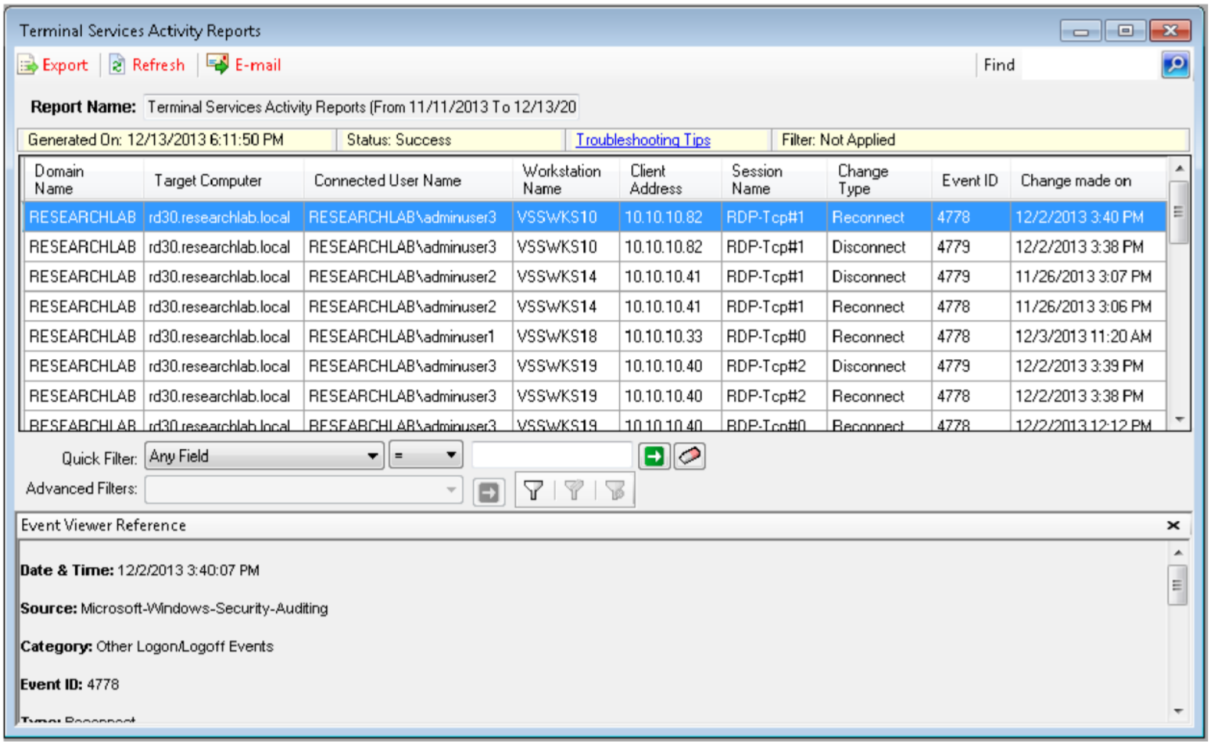
Change type: ☑ Reconnect ☑ Disconnect

3. Specify the Date range, Change type and a field based Filter criteria to find the Terminal Services activity events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Terminal Services Activity Reports (From 11/11/2013 To 12/13/20

Generated On: 12/13/2013 6:11:50 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Target Computer	Connected User Name	Workstation Name	Client Address	Session Name	Change Type	Event ID	Change made on
RESEARCHLAB	rd30.researchlab.local	RESEARCHLAB\adminuser3	VSSWKS10	10.10.10.82	RDP-Tcp#1	Reconnect	4778	12/2/2013 3:40 PM
RESEARCHLAB	rd30.researchlab.local	RESEARCHLAB\adminuser3	VSSWKS10	10.10.10.82	RDP-Tcp#1	Disconnect	4779	12/2/2013 3:38 PM
RESEARCHLAB	rd30.researchlab.local	RESEARCHLAB\adminuser2	VSSWKS14	10.10.10.41	RDP-Tcp#1	Disconnect	4779	11/26/2013 3:07 PM
RESEARCHLAB	rd30.researchlab.local	RESEARCHLAB\adminuser2	VSSWKS14	10.10.10.41	RDP-Tcp#1	Reconnect	4778	11/26/2013 3:06 PM
RESEARCHLAB	rd30.researchlab.local	RESEARCHLAB\adminuser1	VSSWKS18	10.10.10.33	RDP-Tcp#0	Reconnect	4778	12/3/2013 11:20 AM
RESEARCHLAB	rd30.researchlab.local	RESEARCHLAB\adminuser3	VSSWKS19	10.10.10.40	RDP-Tcp#2	Disconnect	4779	12/2/2013 3:39 PM
RESEARCHLAB	rd30.researchlab.local	RESEARCHLAB\adminuser3	VSSWKS19	10.10.10.40	RDP-Tcp#2	Reconnect	4778	12/2/2013 3:38 PM
RESEARCHLAB	rd30.researchlab.local	RESEARCHLAB\adminuser3	VSSWKS19	10.10.10.40	RDP-Tcp#0	Reconnect	4778	12/2/2013 12:12 PM

Quick Filter: Any Field =

Advanced Filters:

Event Viewer Reference

Date & Time: 12/2/2013 3:40:07 PM

Source: Microsoft-Windows-Security-Auditing

Category: Other Logon/Logoff Events

Event ID: 4778

Type: Reconnect

3.4.6 Object Change Reports

Object Change Reports in ADChangeTracker allows you to view events data for any change made to your Active Directory objects since the application is configured for event data collection.

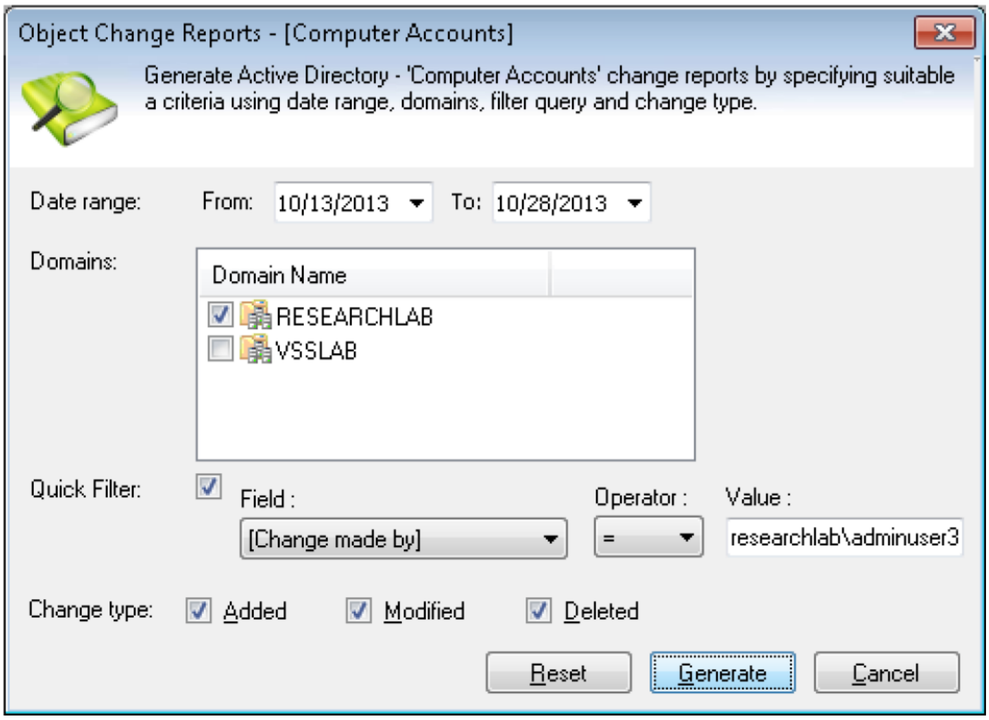
By default, ADChangeTracker collects and reports events data for the following objects only: Builtin-Domain, Computer, Contact, Domain, Domain DNS, Group, Group Policy Container, Organizational Unit, User.

3.4.6.1 How to generate Computer Accounts Change Reports?

To generate the Computer Accounts Change Reports, perform the following steps.

1. Configure settings for 'Object Change Reports' as stated in Configure Events Reports.

2. To launch 'Object Change Reports - [Computer Accounts]' window, click Events Reports -> Object Change Reports -> Computer Accounts... menu in the toolbar. The 'Object Change Reports - [Computer Accounts]' window will appear as shown below:



Object Change Reports - [Computer Accounts]

Generate Active Directory - 'Computer Accounts' change reports by specifying suitable a criteria using date range, domains, filter query and change type.

Date range: From: 10/13/2013 To: 10/28/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

Quick Filter: ☑ Field : [Change made by] Operator : = Value : researchlab\adminuser3

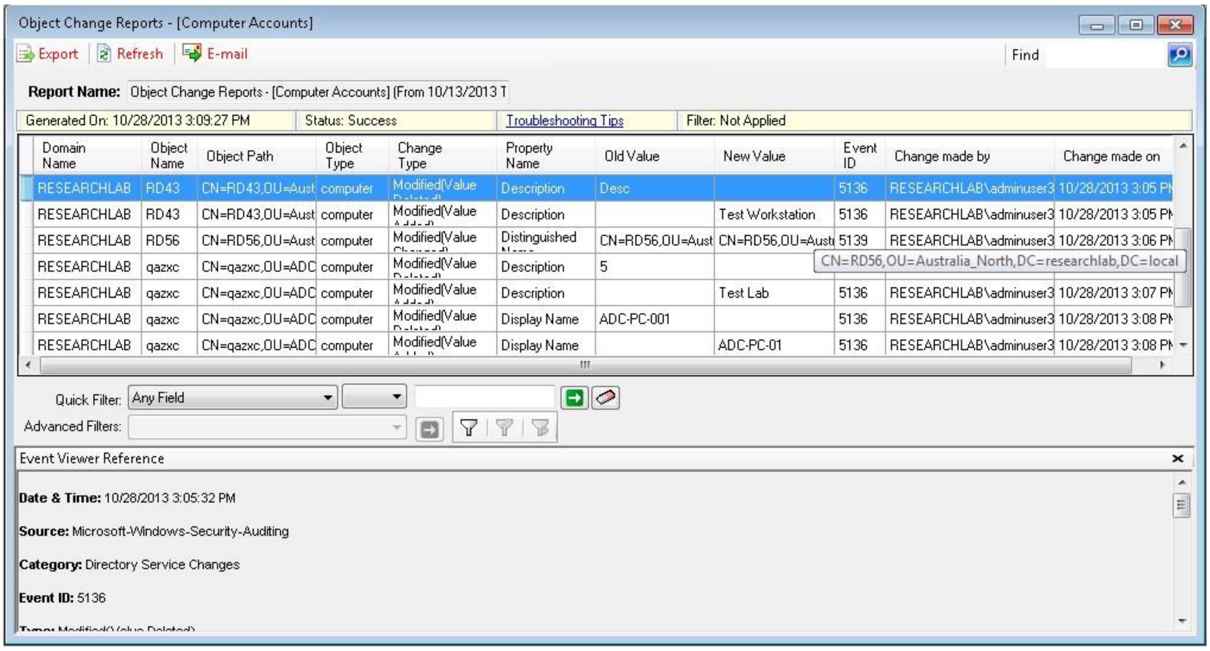
Change type: ☑ Added ☑ Modified ☑ Deleted

3. Specify the Date range, Change type and a field based Filter criteria to find the Computer Accounts change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Object Change Reports - [Computer Accounts]

Report Name: Object Change Reports - [Computer Accounts] (From 10/13/2013 T

Generated On: 10/28/2013 3:09:27 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	RD43	CN=RD43,OU=Aust	computer	Modified(Value	Description	Desc		5136	RESEARCHLAB\adminuser3	10/28/2013 3:05 PI
RESEARCHLAB	RD43	CN=RD43,OU=Aust	computer	Modified(Value	Description		Test Workstation	5136	RESEARCHLAB\adminuser3	10/28/2013 3:05 PI
RESEARCHLAB	RD56	CN=RD56,OU=Aust	computer	Modified(Value	Distinguished	CN=RD56,OU=Aust	CN=RD56,OU=Aust	5139	RESEARCHLAB\adminuser3	10/28/2013 3:06 PI
RESEARCHLAB	qazxc	CN=qazxc,OU=ADC	computer	Modified(Value	Description	5				
RESEARCHLAB	qazxc	CN=qazxc,OU=ADC	computer	Modified(Value	Description		Test Lab	5136	RESEARCHLAB\adminuser3	10/28/2013 3:07 PI
RESEARCHLAB	qazxc	CN=qazxc,OU=ADC	computer	Modified(Value	Display Name	ADC-PC-001		5136	RESEARCHLAB\adminuser3	10/28/2013 3:08 PI
RESEARCHLAB	qazxc	CN=qazxc,OU=ADC	computer	Modified(Value	Display Name		ADC-PC-01	5136	RESEARCHLAB\adminuser3	10/28/2013 3:08 PI

CN=RD56,OU=Australia_North,DC=researchlab,DC=local

Quick Filter: Any Field

Advanced Filters:

Event Viewer Reference

Date & Time: 10/28/2013 3:05:32 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

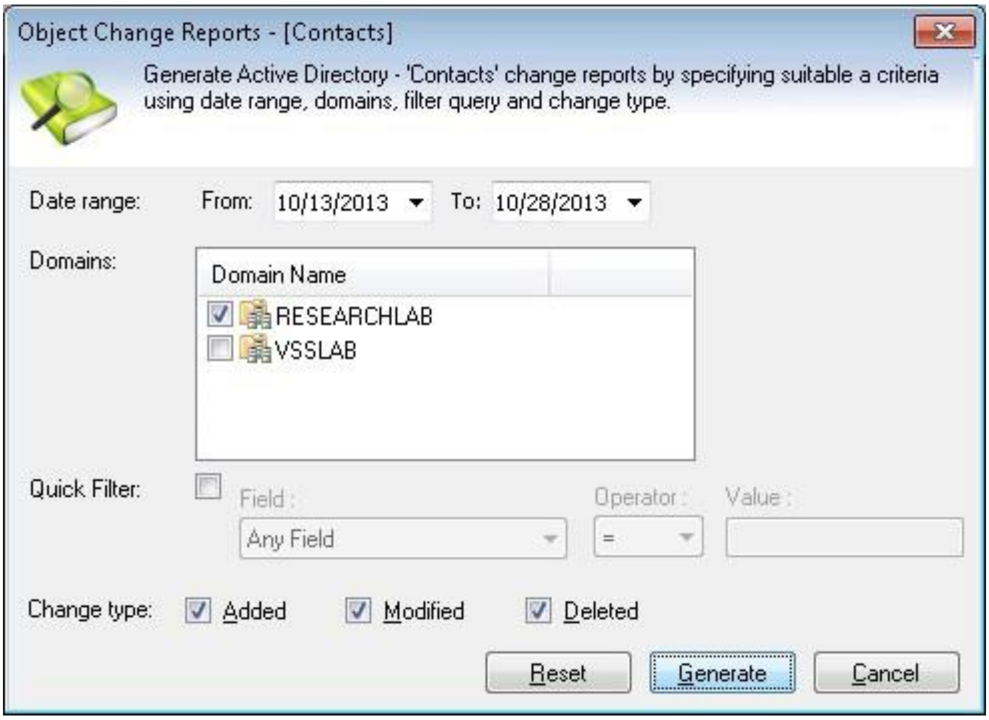
Type: Modified(Value Deleted)

3.4.6.2 How to generate Contacts Change Reports?

To generate the Contacts Change Reports, perform the following the steps.

1. Configure settings for 'Object Change Reports' as stated in Configure Events Reports.

2. To launch 'Object Change Reports - [Contacts]' window, click **Events Reports -> Object Change Reports -> Contacts**... menu in the toolbar. The 'Object Change Reports - [Contacts]' window will appear as shown below:



Object Change Reports - [Contacts]

Generate Active Directory - 'Contacts' change reports by specifying suitable a criteria using date range, domains, filter query and change type.

Date range: From: 10/13/2013 To: 10/28/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

Quick Filter: □ Field : Any Field Operator : = Value :

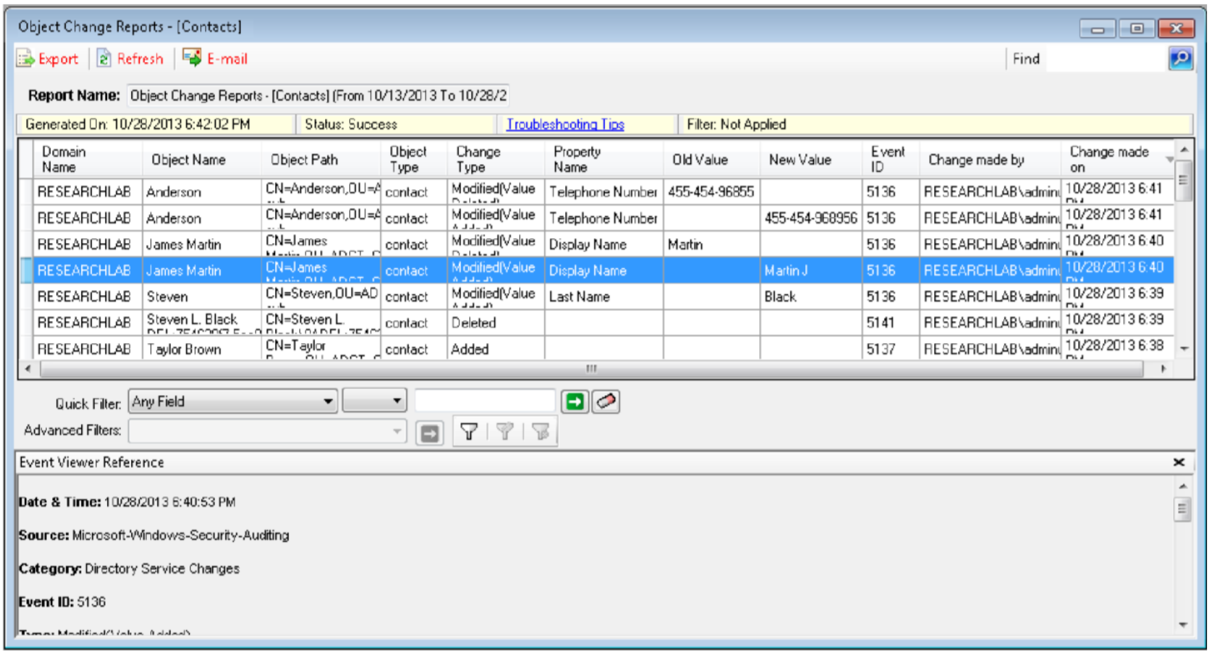
Change type: ☑ Added ☑ Modified ☑ Deleted

3. Specify the Date range, Change type and a field based Filter criteria to find the Contacts change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Object Change Reports - [Contacts]

Report Name: Object Change Reports - [Contacts] (From 10/13/2013 To 10/28/2

Generated On: 10/28/2013 6:42:02 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	Anderson	CN=Anderson,OU=A	contact	Modified(Value	Telephone Number	455-454-96855		5136	RESEARCHLAB\admin	10/28/2013 6:41
RESEARCHLAB	Anderson	CN=Anderson,OU=A	contact	Modified(Value	Telephone Number		455-454-968956	5136	RESEARCHLAB\admin	10/28/2013 6:41
RESEARCHLAB	James Martin	CN=James	contact	Modified(Value	Display Name	Martin		5136	RESEARCHLAB\admin	10/28/2013 6:40
RESEARCHLAB	James Martin	CN=James	contact	Modified(Value	Display Name		Martin J	5136	RESEARCHLAB\admin	10/28/2013 6:40
RESEARCHLAB	Steven	CN=Steven,OU=AD	contact	Modified(Value	Last Name		Black	5136	RESEARCHLAB\admin	10/28/2013 6:39
RESEARCHLAB	Steven L. Black	CN=Steven L.	contact	Deleted				5141	RESEARCHLAB\admin	10/28/2013 6:39
RESEARCHLAB	Taylor Brown	CN=Taylor	contact	Added				5137	RESEARCHLAB\admin	10/28/2013 6:38

Quick Filter: Any Field

Advanced Filters:

Event Viewer Reference

Date & Time: 10/28/2013 6:40:53 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

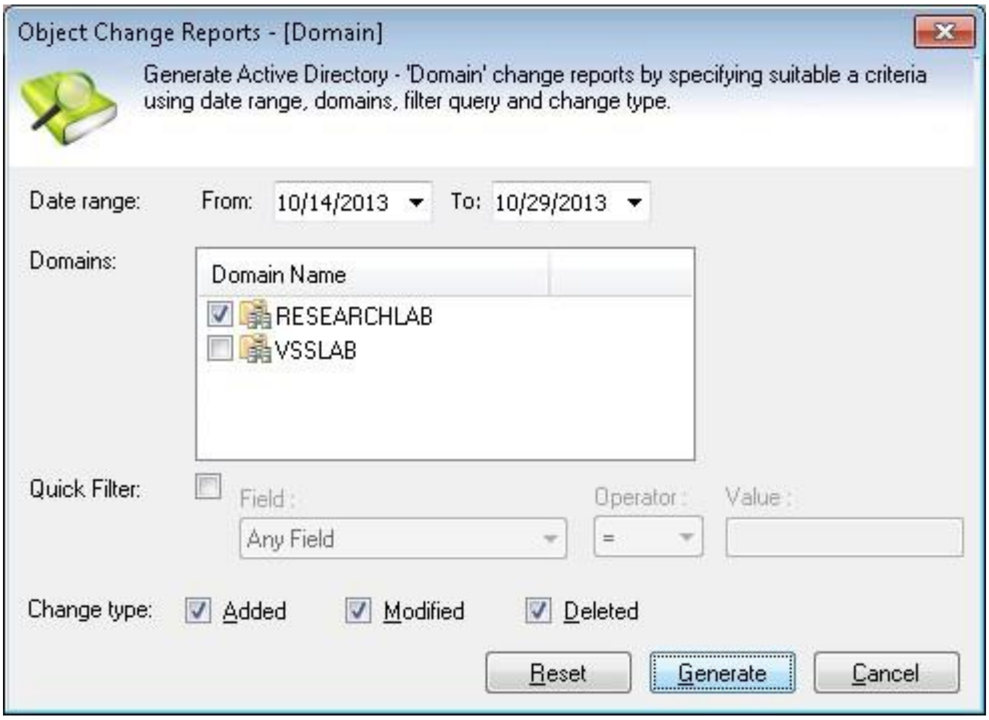
Type: Modified(Value Added)

3.4.6.3 How to generate Domain Change Reports?

To generate the **Domain Change Reports,** perform the following steps.

1. Configure settings for 'Object Change Reports' as stated in Configure Events Reports.

2. To launch 'Object Change Reports - [Domain]' window, click Events Reports -> Object Change Reports -> Domain... menu in the toolbar. The 'Object Change Reports - [Domain]' window will appear as shown below:



Object Change Reports - [Domain]

Generate Active Directory - 'Domain' change reports by specifying suitable a criteria using date range, domains, filter query and change type.

Date range: From: 10/14/2013 To: 10/29/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

Quick Filter: □ Field : Any Field Operator : = Value :

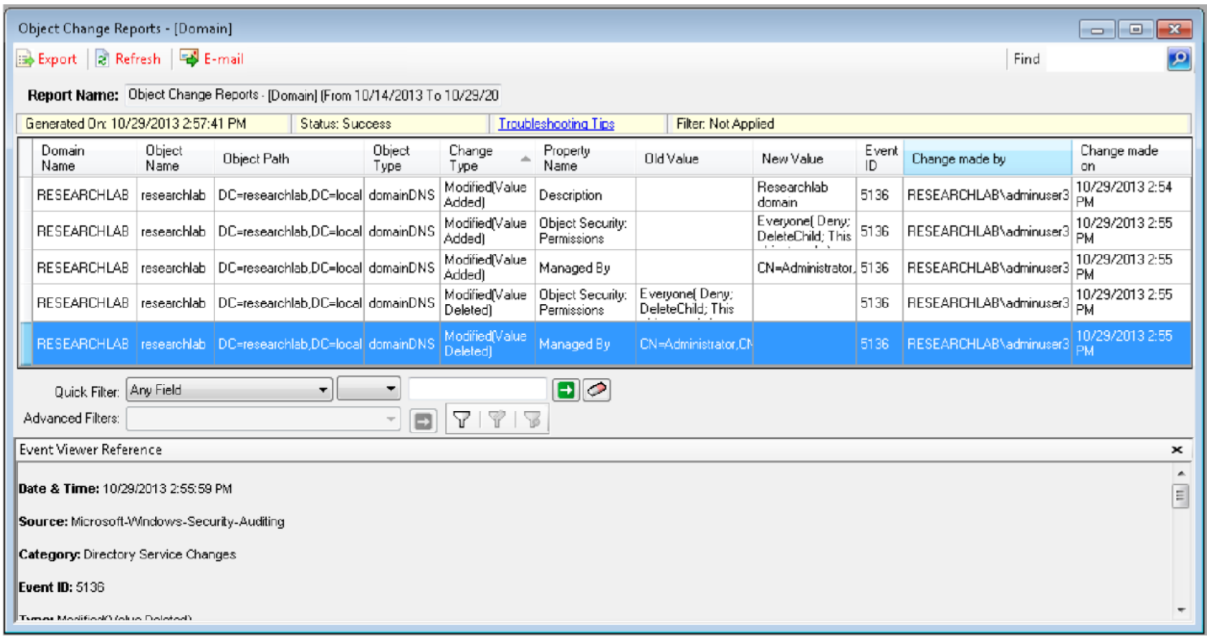
Change type: ☑ Added ☑ Modified ☑ Deleted

3. Specify the Date range, Change type and a field based Filter criteria to find the Domain change events in the application's Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Object Change Reports - [Domain] (From 10/14/2013 To 10/29/20

Generated On: 10/29/2013 2:57:41 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	researchlab	DC=researchlab,DC=local	domainDNS	Modified(Value Added)	Description		Researchlab domain	5136	RESEARCHLAB\adminuser3	10/29/2013 2:54 PM
RESEARCHLAB	researchlab	DC=researchlab,DC=local	domainDNS	Modified(Value Added)	Object Security: Permissions		Everyone(Deny; DeleteChild; This	5136	RESEARCHLAB\adminuser3	10/29/2013 2:55 PM
RESEARCHLAB	researchlab	DC=researchlab,DC=local	domainDNS	Modified(Value Added)	Managed By		CN=Administrator,	5136	RESEARCHLAB\adminuser3	10/29/2013 2:55 PM
RESEARCHLAB	researchlab	DC=researchlab,DC=local	domainDNS	Modified(Value Deleted)	Object Security: Permissions	Everyone(Deny; DeleteChild; This		5136	RESEARCHLAB\adminuser3	10/29/2013 2:55 PM
RESEARCHLAB	researchlab	DC=researchlab,DC=local	domainDNS	Modified(Value Deleted)	Managed By	CN=Administrator,CN		5136	RESEARCHLAB\adminuser3	10/29/2013 2:55 PM

Quick Filter: Any Field

Advanced Filters:

Event Viewer Reference

Date & Time: 10/29/2013 2:55:59 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

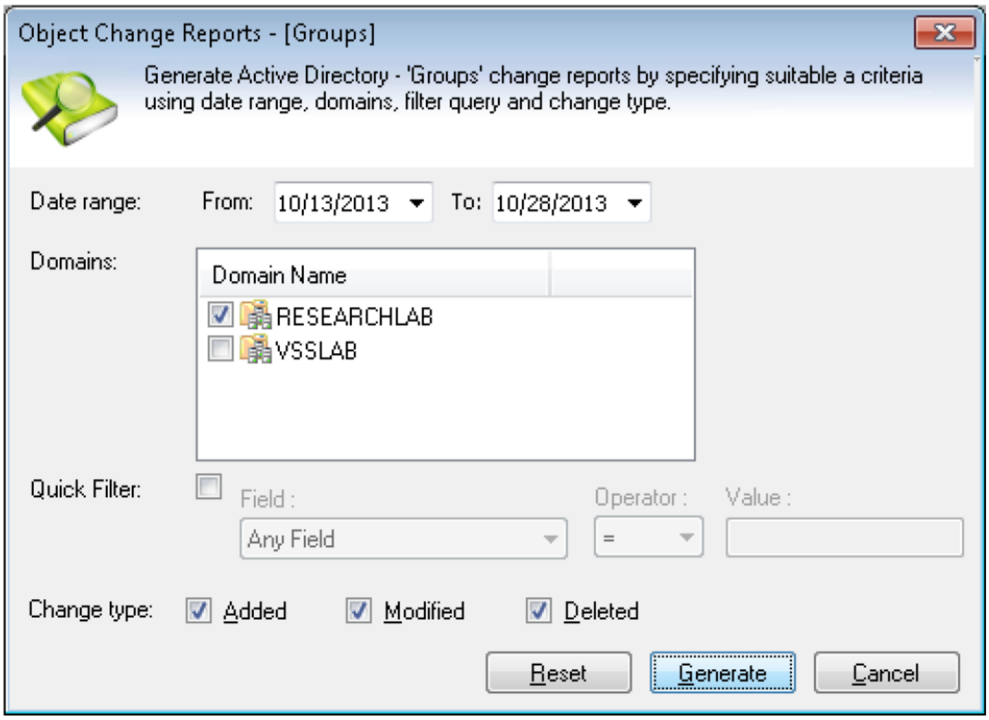
Event ID: 5136

Type: Modified(Value Deleted)

3.4.6.4 How to generate Groups Change Reports?

To generate the Groups Change Reports, perform the following steps.

1. Configure settings for 'Object Change Reports' as stated in Configure Events Reports.
2. To launch 'Object Change Reports - [Groups]' window, click Events Reports -> Object Change Reports -> Groups... menu in the toolbar. The 'Object Change Reports - [Groups]' window will appear as shown below:



Object Change Reports - [Groups]

Generate Active Directory - 'Groups' change reports by specifying suitable a criteria using date range, domains, filter query and change type.

Date range: From: 10/13/2013 To: 10/28/2013

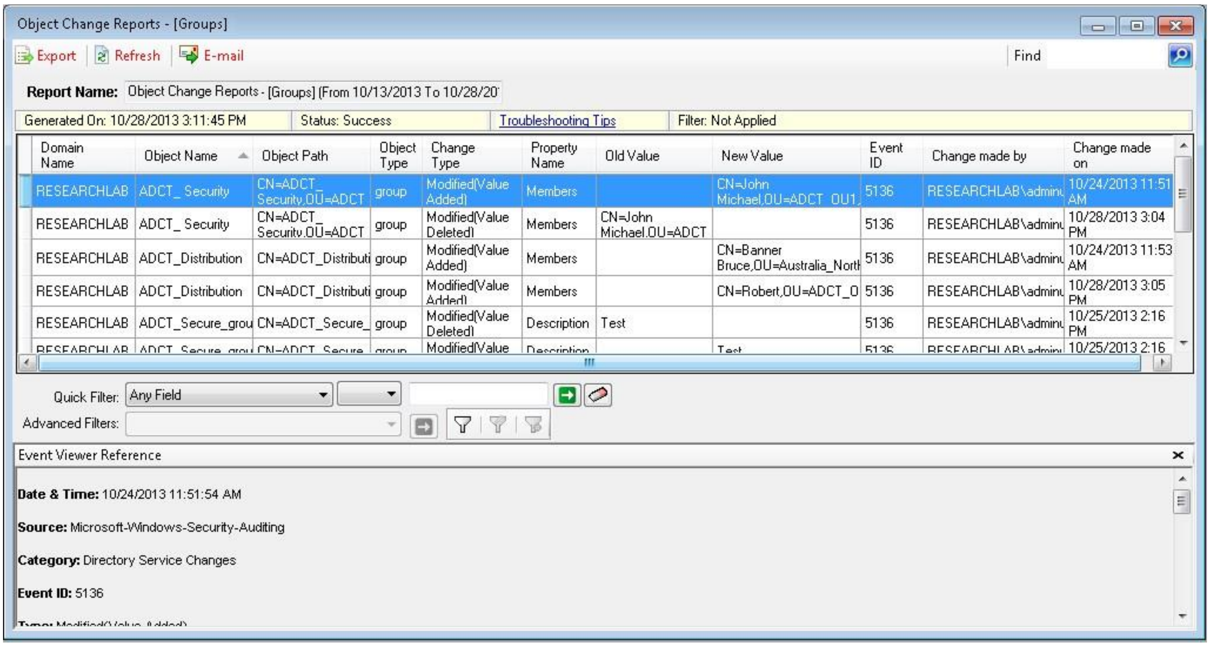
Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

Quick Filter: □ Field : Any Field Operator : = Value :

Change type: ☑ Added ☑ Modified ☑ Deleted

3. Specify the Date range, Change type and a field based Filter criteria to find the Groups change events in the application’s Events History database.
4. Select the desired Domains to generate your reports on.
5. Click Generate button to generate the report.
6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Object Change Reports - [Groups] (From 10/13/2013 To 10/28/20

Generated On: 10/28/2013 3:11:45 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	ADCT_ Security	CN=ADCT_ Security,OU=ADCT	group	Modified(Value Added)	Members		CN=John Michael,OU=ADCT_OU1,	5136	RESEARCHLAB\adminu	10/24/2013 11:51 AM
RESEARCHLAB	ADCT_ Security	CN=ADCT_ Security,OU=ADCT	group	Modified(Value Deleted)	Members	CN=John Michael,OU=ADCT		5136	RESEARCHLAB\adminu	10/28/2013 3:04 PM
RESEARCHLAB	ADCT_Distribution	CN=ADCT_Distributi	group	Modified(Value Added)	Members		CN=Banner Bruce,OU=Australia_Nortl	5136	RESEARCHLAB\adminu	10/24/2013 11:53 AM
RESEARCHLAB	ADCT_Distribution	CN=ADCT_Distributi	group	Modified(Value Added)	Members		CN=Robert,OU=ADCT_O	5136	RESEARCHLAB\adminu	10/28/2013 3:05 PM
RESEARCHLAB	ADCT_Secure_grou	CN=ADCT_Secure_	group	Modified(Value Deleted)	Description	Test		5136	RESEARCHLAB\adminu	10/25/2013 2:16 PM
RESEARCHLAB	ADCT_Secure_grou	CN=ADCT_Secure_	group	Modified(Value	Description		Test	5136	RESEARCHLAB\admin	10/25/2013 2:16

Quick Filter: Any Field

Advanced Filters:

Event Viewer Reference

Date & Time: 10/24/2013 11:51:54 AM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

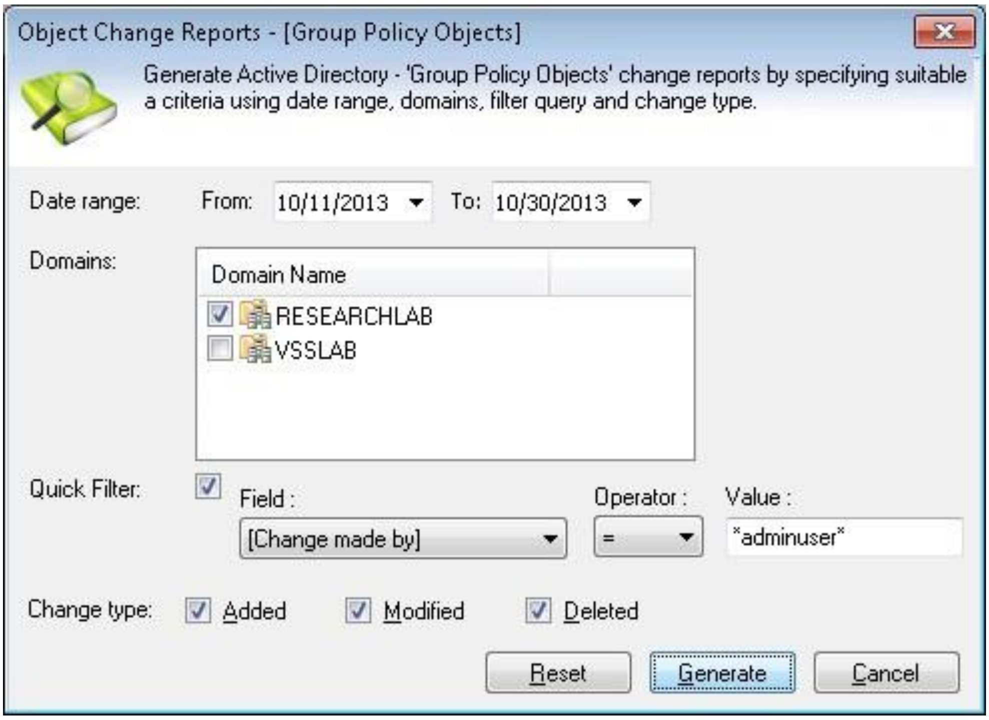
Event ID: 5136

Type: Modified(Value Added)

3.4.6.5 How to generate Group Policy Objects Change Reports?

To generate the **Group Policy Objects Change Reports,** perform the following steps.

1. Configure settings for 'Object Change Reports' as stated in Configure Events Reports.
2. To launch 'Object Change Reports - [Group Policy Objects]' window, click Events Reports -> Object Change Reports -> Group Policy Objects... menu in the toolbar. The 'Object Change Reports - [Group Policy Objects]' window will appear as shown below:



Object Change Reports - [Group Policy Objects]

Generate Active Directory - 'Group Policy Objects' change reports by specifying suitable a criteria using date range, domains, filter query and change type.

Date range: From: 10/11/2013 To: 10/30/2013

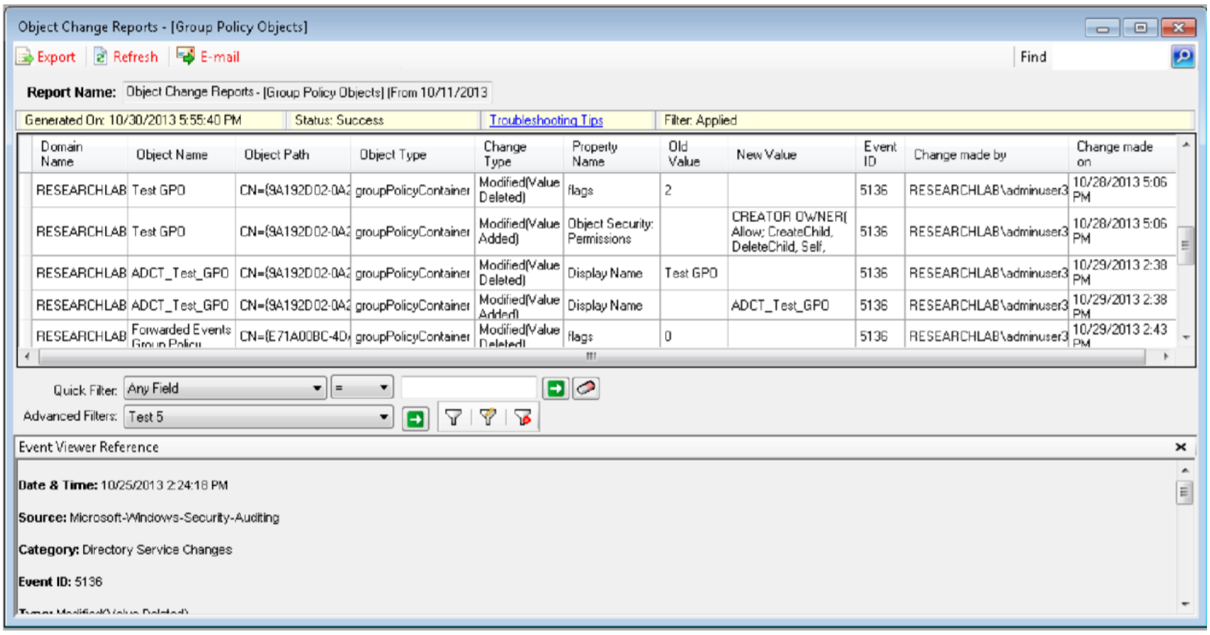
Domains:

Domain Name
☑ RESEARCHLAB
☐ VSSLAB

Quick Filter: ☑ Field : [Change made by] Operator : = Value : *adminuser*

Change type: ☑ Added ☑ Modified ☑ Deleted

3. Specify the Date range, Change type and a field based Filter criteria to find the Group Policy Objects change events in the application’s Events History database.
4. Select the desired Domains to generate your reports on.
5. Click Generate button to generate the report.
6. Once the data collection is complete, the report will be generated in a report window as shown below:



Object Change Reports - [Group Policy Objects]

Report Name: Object Change Reports - [Group Policy Objects] [From 10/11/2013

Generated On: 10/30/2013 5:55:40 PM | Status: Success | Troubleshooting Tips | Filter: Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	Test GPO	CN={9A192D02-0A2	groupPolicyContainer	Modified(Value Deleted)	flags	2		5136	RESEARCHLAB\adminuser3	10/28/2013 5:06 PM
RESEARCHLAB	Test GPO	CN={9A192D02-0A2	groupPolicyContainer	Modified(Value Added)	Object Security: Permissions		CREATOR OWNER(Allow; CreateChild, DeleteChild, Self,	5136	RESEARCHLAB\adminuser3	10/28/2013 5:06 PM
RESEARCHLAB	ADCT_Test_GPO	CN={9A192D02-0A2	groupPolicyContainer	Modified(Value Deleted)	Display Name	Test GPO		5136	RESEARCHLAB\adminuser3	10/29/2013 2:38 PM
RESEARCHLAB	ADCT_Test_GPO	CN={9A192D02-0A2	groupPolicyContainer	Modified(Value Added)	Display Name		ADCT_Test_GPO	5136	RESEARCHLAB\adminuser3	10/29/2013 2:38 PM
RESEARCHLAB	Forwarded Events Group Policy	CN={E71A00BC-4D	groupPolicyContainer	Modified(Value Deleted)	flags	0		5136	RESEARCHLAB\adminuser3	10/29/2013 2:43 PM

Quick Filter: Any Field | = |

Advanced Filters: Test 5

Event Viewer Reference

Date & Time: 10/25/2013 2:24:18 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

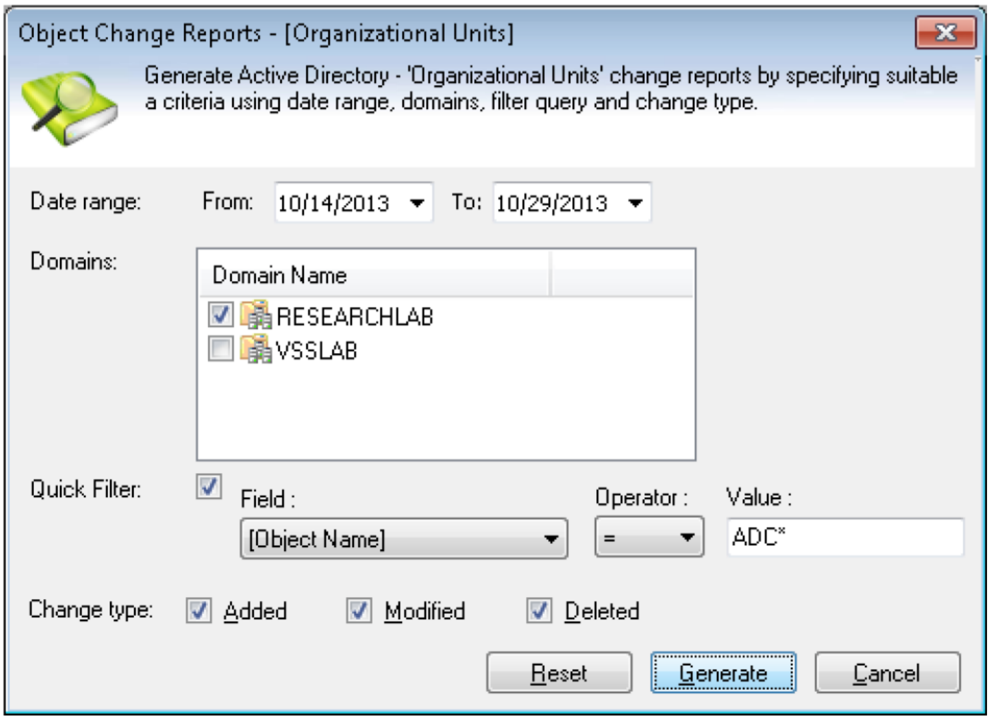
Type: Modified(Value Deleted)

3.4.6.6 How to generate Organizational Units Change Reports?

To generate the Organizational Units Change Reports, perform the following steps.

1. Configure settings 'Object Change Reports' as stated in Configure Events Reports.

2. To launch 'Object Change Reports - [Organizational Units]' window, click Events Reports -> Object Change Reports -> Organizational Units... menu in the toolbar. The 'Object Change Reports - [Organizational Units]' window will appear as shown below:



Object Change Reports - [Organizational Units]

Generate Active Directory - 'Organizational Units' change reports by specifying suitable a criteria using date range, domains, filter query and change type.

Date range: From: 10/14/2013 To: 10/29/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

Quick Filter: ☑ Field : [Object Name] Operator : = Value : ADC*

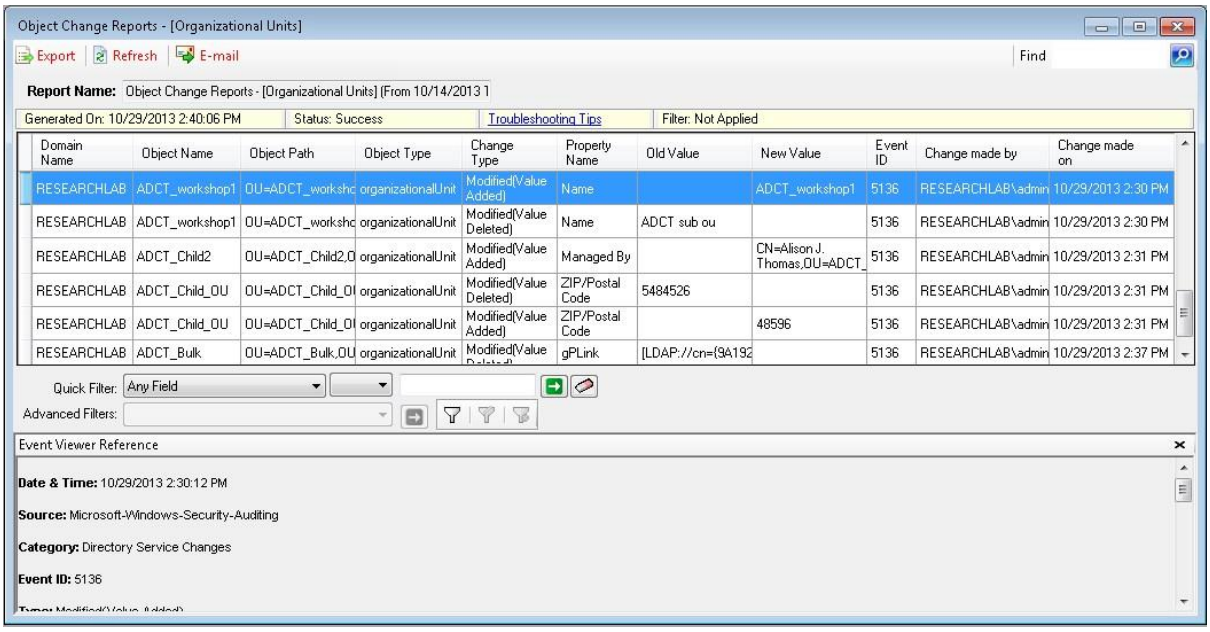
Change type: ☑ Added ☑ Modified ☑ Deleted

3. Specify the Date range, Change type and a field based Filter criteria to find the Organizational Units change events in the application's Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Object Change Reports - [Organizational Units]

Report Name: Object Change Reports - [Organizational Units] (From 10/14/2013 1

Generated On: 10/29/2013 2:40:06 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	ADCT_workshop1	OU=ADCT_workshc	organizationalUnit	Modified(Value Added)	Name		ADCT_workshop1	5136	RESEARCHLAB\admin	10/29/2013 2:30 PM
RESEARCHLAB	ADCT_workshop1	OU=ADCT_workshc	organizationalUnit	Modified(Value Deleted)	Name	ADCT sub ou		5136	RESEARCHLAB\admin	10/29/2013 2:30 PM
RESEARCHLAB	ADCT_Child2	OU=ADCT_Child2,O	organizationalUnit	Modified(Value Added)	Managed By		CN=Alison J. Thomas,OU=ADCT_	5136	RESEARCHLAB\admin	10/29/2013 2:31 PM
RESEARCHLAB	ADCT_Child_OU	OU=ADCT_Child_OI	organizationalUnit	Modified(Value Deleted)	ZIP/Postal Code	5484526		5136	RESEARCHLAB\admin	10/29/2013 2:31 PM
RESEARCHLAB	ADCT_Child_OU	OU=ADCT_Child_OI	organizationalUnit	Modified(Value Added)	ZIP/Postal Code		48596	5136	RESEARCHLAB\admin	10/29/2013 2:31 PM
RESEARCHLAB	ADCT_Bulk	OU=ADCT_Bulk,OU	organizationalUnit	Modified(Value	gPLink	[LDAP://cn={9A192		5136	RESEARCHLAB\admin	10/29/2013 2:37 PM

Quick Filter: Any Field

Advanced Filters:

Event Viewer Reference

Date & Time: 10/29/2013 2:30:12 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

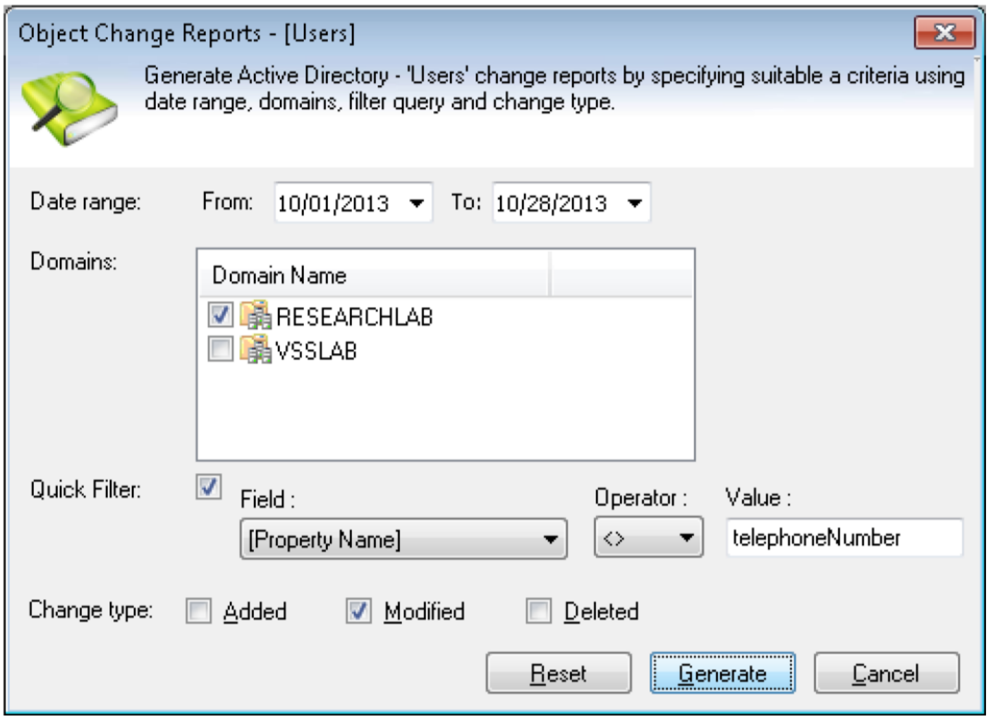
Type: Modified(Value Added)

3.4.6.7 How to generate Users Change Reports?

To generate the Users Change Reports, perform the following steps.

1. Configure settings 'Object Change Reports' as stated in Configure Events Reports.

2. To launch 'Object Change Reports - [Users]' window, click Events Reports -> Object Change Reports -> Users... menu in the toolbar. The 'Object Change Reports - [Users]' window will appear as shown below:



Object Change Reports - [Users]

Generate Active Directory - 'Users' change reports by specifying suitable a criteria using date range, domains, filter query and change type.

Date range: From: 10/01/2013 To: 10/28/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

Quick Filter: ☑ Field : [Property Name] Operator : <> Value : telephoneNumber

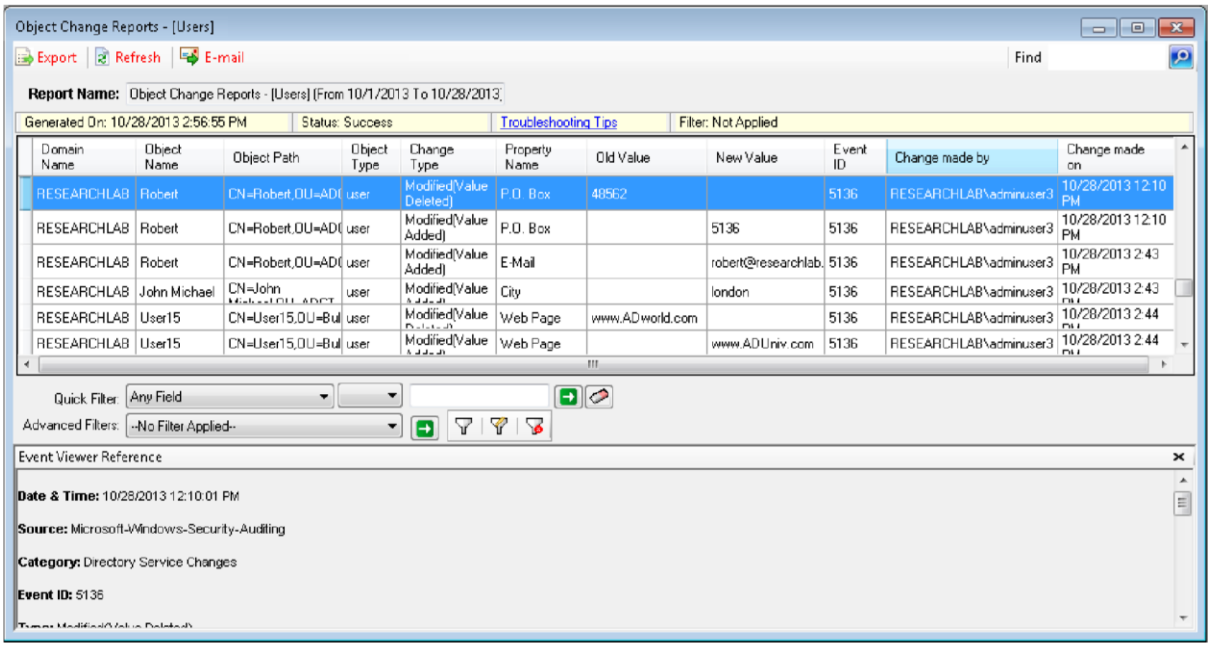
Change type: □ Added ☑ Modified □ Deleted

3. Specify the Date range, Change type and a field based Filter criteria to find the Users change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Object Change Reports - [Users]

Report Name: Object Change Reports - [Users] (From 10/1/2013 To 10/28/2013

Generated On: 10/28/2013 2:56:55 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	Robert	CN=Robert,OU=AD(	user	Modified(Value Deleted)	P.O. Box	48562		5136	RESEARCHLAB\adminuser3	10/28/2013 12:10 PM
RESEARCHLAB	Robert	CN=Robert,OU=AD(	user	Modified(Value Added)	P.O. Box		5136	5136	RESEARCHLAB\adminuser3	10/28/2013 12:10 PM
RESEARCHLAB	Robert	CN=Robert,OU=AD(	user	Modified(Value Added)	E-Mail		robert@researchlab.	5136	RESEARCHLAB\adminuser3	10/28/2013 2:43 PM
RESEARCHLAB	John Michael	CN=John	user	Modified(Value	City		london	5136	RESEARCHLAB\adminuser3	10/28/2013 2:43
RESEARCHLAB	User15	CN=User15,OU=Bul	user	Modified(Value	Web Page	www.ADworld.com		5136	RESEARCHLAB\adminuser3	10/28/2013 2:44
RESEARCHLAB	User15	CN=User15,OU=Bul	user	Modified(Value	Web Page		www.ADUniv.com	5136	RESEARCHLAB\adminuser3	10/28/2013 2:44

Quick Filter: Any Field

Advanced Filters: --No Filter Applied--

Event Viewer Reference

Date & Time: 10/28/2013 12:10:01 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

Type: Modified(Value Deleted)

3.4.7 Permissions Change Reports

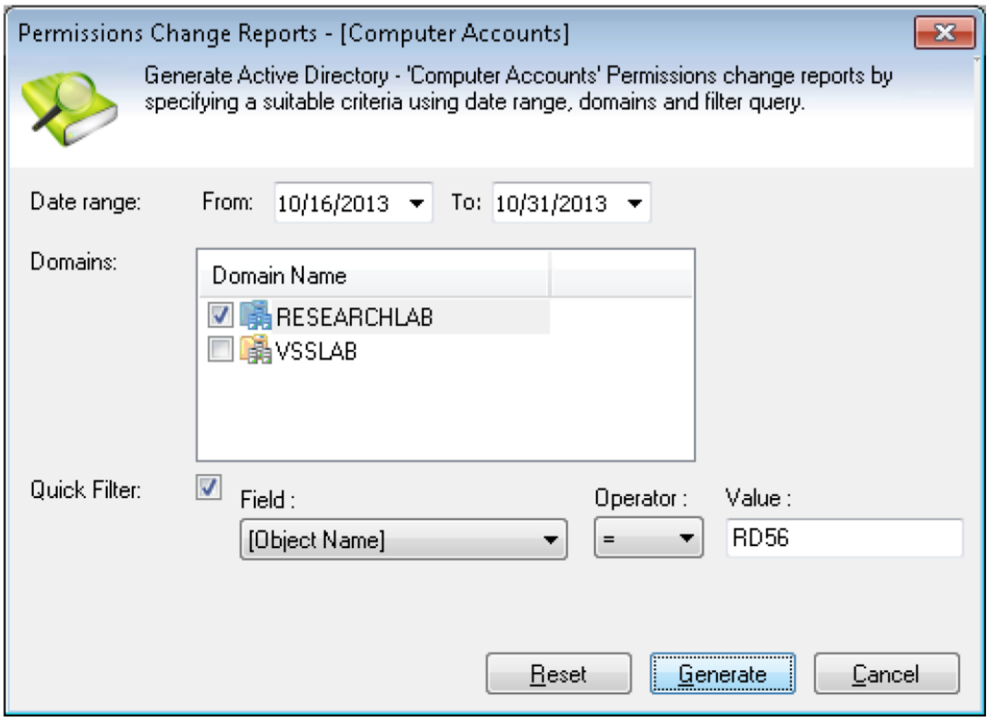
Permissions Change Reports in ADChangeTracker allows you to view events data for Permissions changes made to your Active Directory objects since the application is configured for event data collection.

By default, ADChangeTracker collects and reports events data for the following objects only: Builtin-Domain, Computer, Contact, Domain, Domain DNS, Group, Group Policy Container, Organizational Unit, User.

3.4.7.1 How to generate Computer Accounts Permissions

To generate the Computer Accounts Permissions Change Reports, perform the following steps.

1. Configure settings for 'Permissions Change Reports' as stated in Configure Events Reports.
2. To launch 'Permissions Change Reports - [Computer Accounts]' window, click Events Reports -> Permissions Change Reports -> Computer Accounts... menu in the toolbar. The 'Permissions Change Reports - [Computer Accounts]' window will appear as shown below:



Permissions Change Reports - [Computer Accounts]

Generate Active Directory - 'Computer Accounts' Permissions change reports by specifying a suitable criteria using date range, domains and filter query.

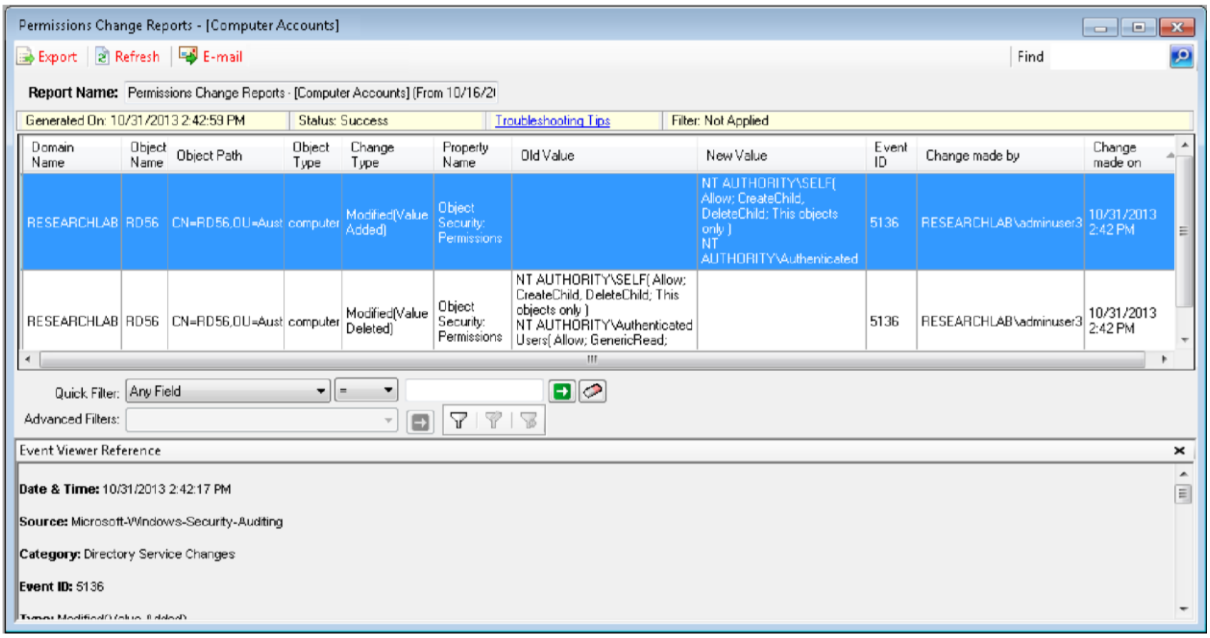
Date range: From: 10/16/2013 To: 10/31/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

Quick Filter: ☑ Field : [Object Name] Operator : = Value : RD56

3. Specify the Date range and a field based Filter criteria to find the Computer Accounts Permissions change events in the application’s Events History database.
4. Select the desired Domains to generate your reports on.
5. Click Generate button to generate the report.
6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Permissions Change Reports - [Computer Accounts] [From 10/16/2

Generated On: 10/31/2013 2:42:59 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	RD56	CN=RD56,OU=Aust	computer	Modified(Value Added)	Object Security: Permissions		NT AUTHORITY\SELF(Allow; CreateChild, DeleteChild; This objects only) NT AUTHORITY\Authenticated	5136	RESEARCHLAB\adminuser3	10/31/2013 2:42 PM
RESEARCHLAB	RD56	CN=RD56,OU=Aust	computer	Modified(Value Deleted)	Object Security: Permissions	NT AUTHORITY\SELF(Allow; CreateChild, DeleteChild; This objects only) NT AUTHORITY\Authenticated Users(Allow; GenericRead;		5136	RESEARCHLAB\adminuser3	10/31/2013 2:42 PM

Date & Time: 10/31/2013 2:42:17 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

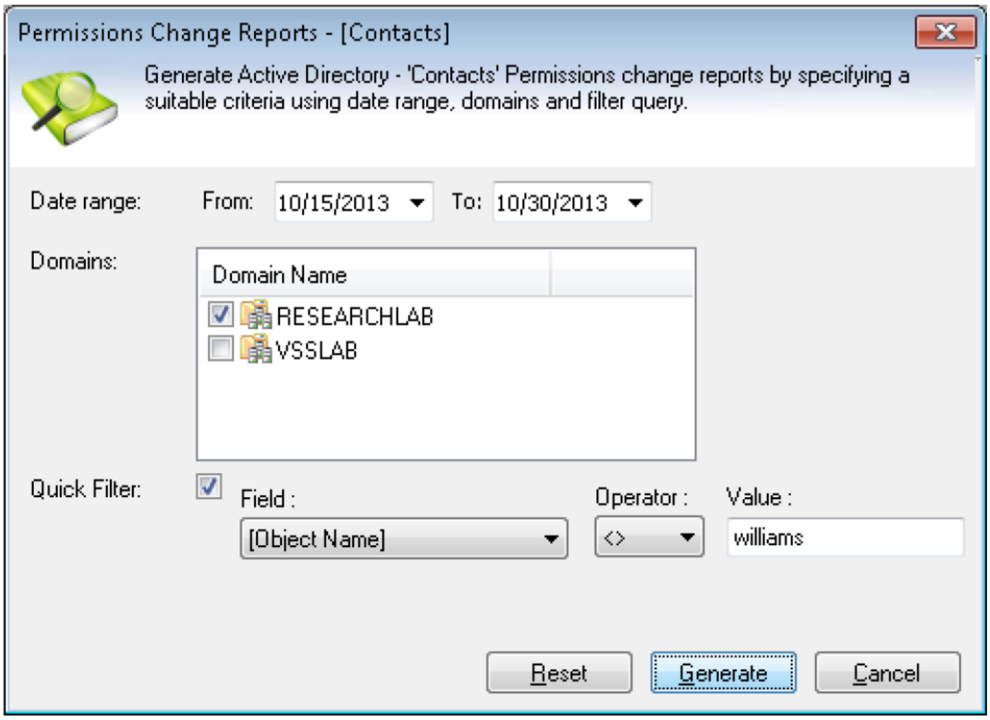
Type: Modified(Value Added)

3.4.7.2 How to generate Contacts Permissions Change Reports?

To generate the Contacts Permissions Change Reports, perform the following steps.

1. Configure settings for 'Permissions Change Reports' as stated in Configure Events Reports.

2. To launch 'Permissions Change Reports - [Contacts]' window, click Events Reports -> Permissions Change Reports -> Contacts... menu in the toolbar. The 'Permissions Change Reports - [Contacts]' window will appear as shown below:



Permissions Change Reports - [Contacts]

Generate Active Directory - 'Contacts' Permissions change reports by specifying a suitable criteria using date range, domains and filter query.

Date range: From: 10/15/2013 To: 10/30/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

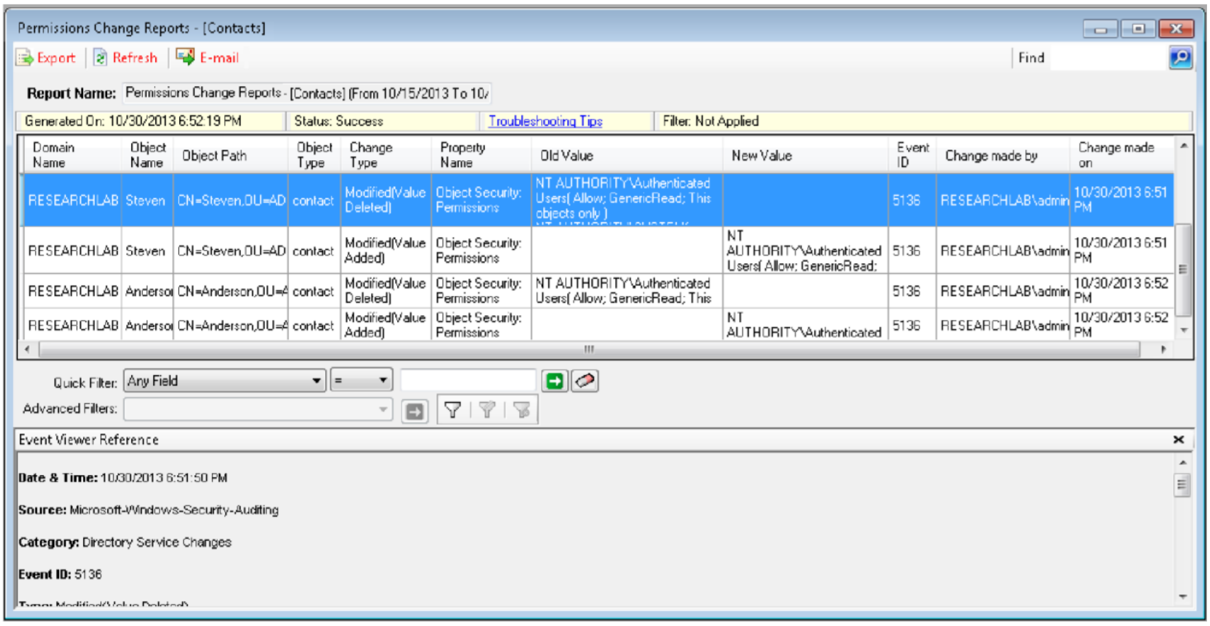
Quick Filter: ☑ Field : [Object Name] Operator : <> Value : williams

3. Specify the Date range and a field based Filter criteria to find the Contacts Permissions change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Permissions Change Reports - [Contacts] (From 10/15/2013 To 10/

Generated On: 10/30/2013 6:52:19 PM | Status: Success | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	Steven	CN=Steven,OU=AD	contact	Modified(Value Deleted)	Object Security: Permissions	NT AUTHORITY\Authenticated Users(Allow; GenericRead; This objects only)		5136	RESEARCHLAB\admin	10/30/2013 6:51 PM
RESEARCHLAB	Steven	CN=Steven,OU=AD	contact	Modified(Value Added)	Object Security: Permissions		NT AUTHORITY\Authenticated Users(Allow; GenericRead;	5136	RESEARCHLAB\admin	10/30/2013 6:51 PM
RESEARCHLAB	Andersoı	CN=Anderson,OU=A	contact	Modified(Value Deleted)	Object Security: Permissions	NT AUTHORITY\Authenticated Users(Allow; GenericRead; This		5136	RESEARCHLAB\admin	10/30/2013 6:52 PM
RESEARCHLAB	Andersoı	CN=Anderson,OU=A	contact	Modified(Value Added)	Object Security: Permissions		NT AUTHORITY\Authenticated	5136	RESEARCHLAB\admin	10/30/2013 6:52 PM

Quick Filter: Any Field =

Date & Time: 10/30/2013 6:51:50 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

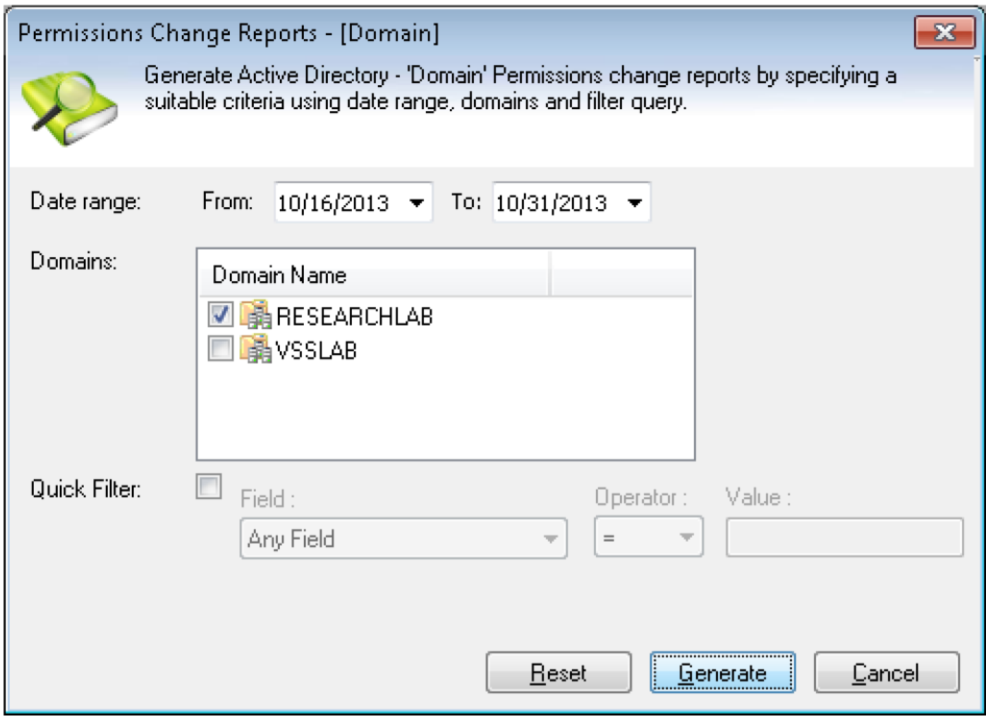
Type: Modified(Value Deleted)

3.4.7.3 How to generate Domain Permissions Change Reports?

To generate the **Domain Permissions Change Reports,** perform the following steps.

1. Configure settings for 'Permissions Change Reports' as stated in Configure Events Reports.

2. To launch 'Permissions Change Reports - [Domain]' window, click Events Reports -> Permissions Change Reports -> Domain... menu in the toolbar. The 'Permissions Change Reports - [Domain]' window will appear as shown below:



Permissions Change Reports - [Domain]

Generate Active Directory - 'Domain' Permissions change reports by specifying a suitable criteria using date range, domains and filter query.

Date range: From: 10/16/2013 To: 10/31/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

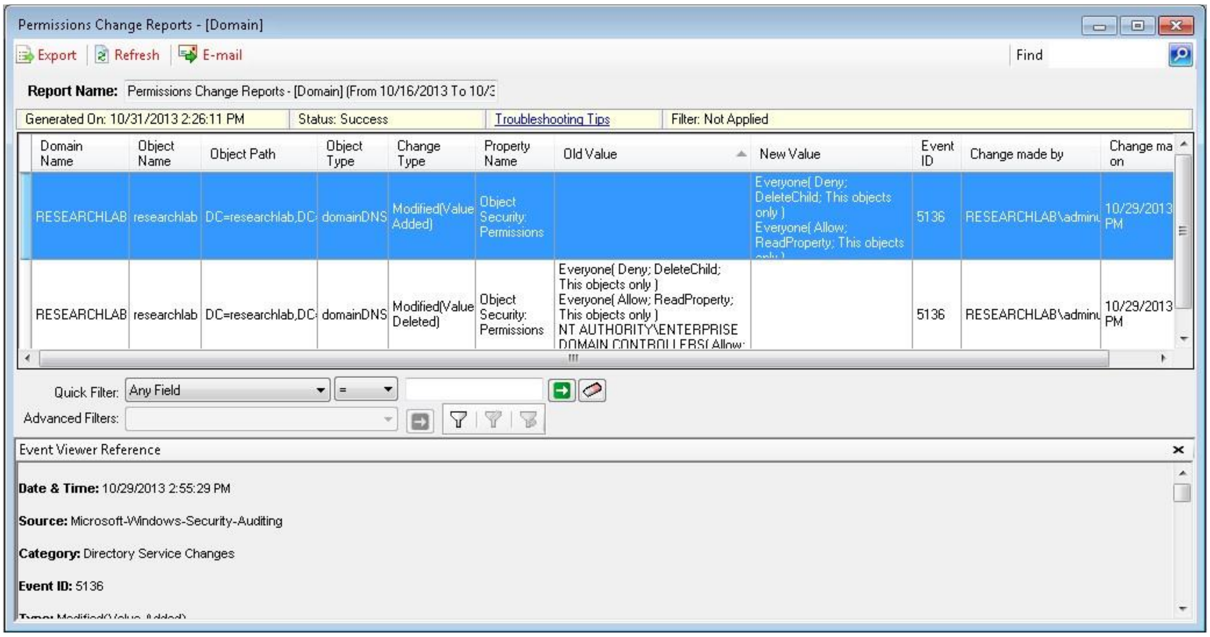
Quick Filter: □ Field : Any Field Operator : = Value :

3. Specify the Date range and a field based Filter criteria to find the Domain Permissions change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Permissions Change Reports - [Domain] (From 10/16/2013 To 10/3

Generated On: 10/31/2013 2:26:11 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change ma on

RESEARCHLAB	researchlab	DC=researchlab,DC	domainDNS	Modified(Value Added)	Object Security: Permissions		Everyone(Deny; DeleteChild; This objects only)
							Everyone(Allow; ReadProperty; This objects only)
								5136	RESEARCHLAB\adminu	10/29/2013 PM

RESEARCHLAB	researchlab	DC=researchlab,DC	domainDNS	Modified(Value Deleted)	Object Security: Permissions	Everyone(Deny; DeleteChild; This objects only)
						Everyone(Allow; ReadProperty; This objects only)
						NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS(Allow;
								5136	RESEARCHLAB\adminu	10/29/2013 PM

Quick Filter: Any Field =

Advanced Filters:

Event Viewer Reference

Date & Time: 10/29/2013 2:55:29 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

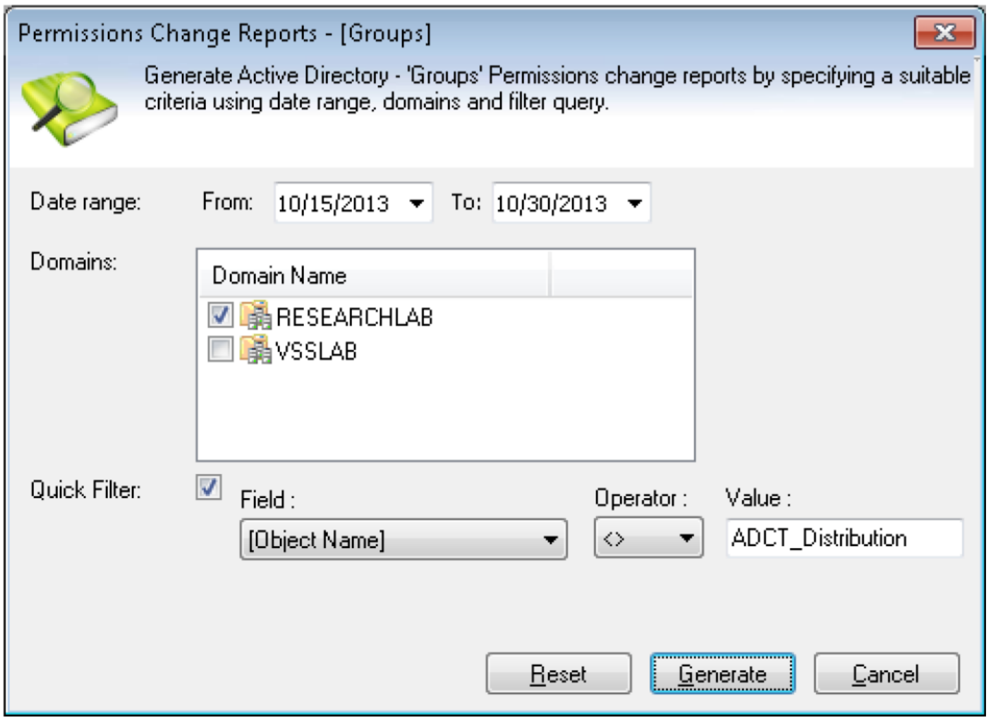
Type: Modified(Value Added)

3.4.7.4 How to generate Groups Permissions Change Reports?

To generate the **Groups Permissions Change Reports,** perform the following steps.

1. Configure settings for 'Permissions Change Reports' as stated in Configure Events Reports.

2. To launch 'Permissions Change Reports - [Groups]' window, click Events Reports > Permissions Change Reports -> Groups... menu in the toolbar. The 'Permissions Change Reports - [Groups]' window will appear as shown below:



Permissions Change Reports - [Groups]

Generate Active Directory - 'Groups' Permissions change reports by specifying a suitable criteria using date range, domains and filter query.

Date range: From: 10/15/2013 To: 10/30/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

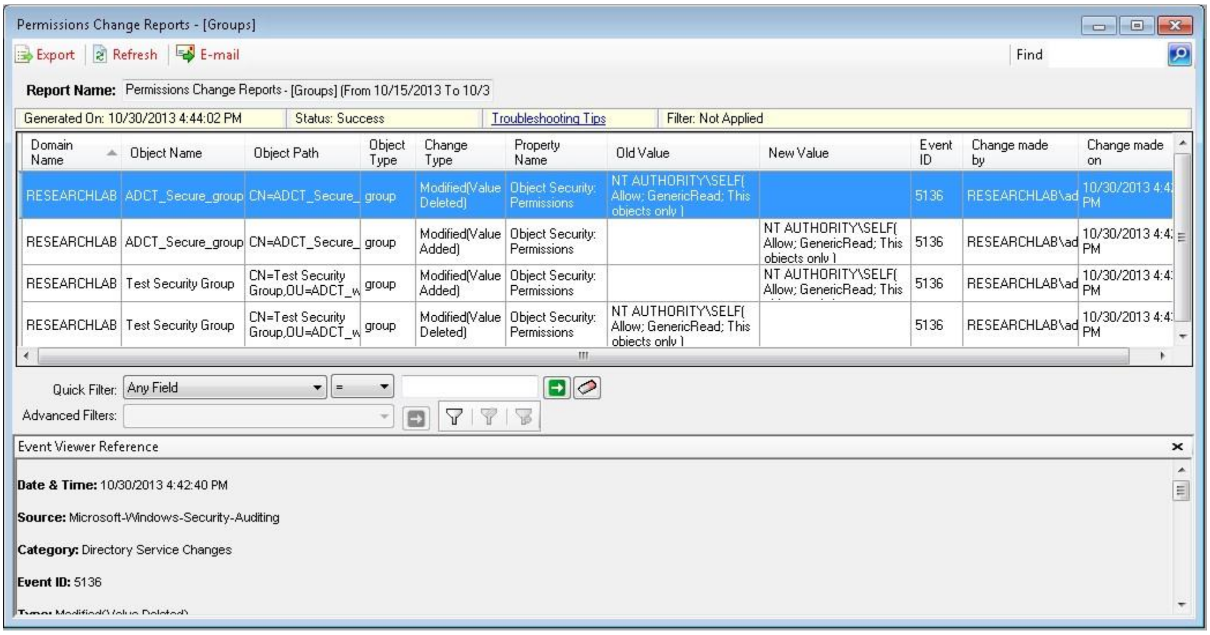
Quick Filter: ☑ Field : [Object Name] Operator : <> Value : ADCT_Distribution

3. Specify the Date range and a field based Filter criteria to find the Groups Permissions change events in the application's Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report would be generated in a report window as shown below:



Permissions Change Reports - [Groups]

Report Name: Permissions Change Reports - [Groups] (From 10/15/2013 To 10/3

Generated On: 10/30/2013 4:44:02 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	ADCT_Secure_group	CN=ADCT_Secure_	group	Modified(Value Deleted)	Object Security: Permissions	NT AUTHORITY\SELF(Allow; GenericRead; This objects only)		5136	RESEARCHLAB\ad	10/30/2013 4:4 PM
RESEARCHLAB	ADCT_Secure_group	CN=ADCT_Secure_	group	Modified(Value Added)	Object Security: Permissions		NT AUTHORITY\SELF(Allow; GenericRead; This objects only)	5136	RESEARCHLAB\ad	10/30/2013 4:4 PM
RESEARCHLAB	Test Security Group	CN=Test Security Group,OU=ADCT_w	group	Modified(Value Added)	Object Security: Permissions		NT AUTHORITY\SELF(Allow; GenericRead; This	5136	RESEARCHLAB\ad	10/30/2013 4:4 PM
RESEARCHLAB	Test Security Group	CN=Test Security Group,OU=ADCT_w	group	Modified(Value Deleted)	Object Security: Permissions	NT AUTHORITY\SELF(Allow; GenericRead; This objects only)		5136	RESEARCHLAB\ad	10/30/2013 4:4 PM

Quick Filter: Any Field =

Advanced Filters:

Event Viewer Reference

Date & Time: 10/30/2013 4:42:40 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Changes

Event ID: 5136

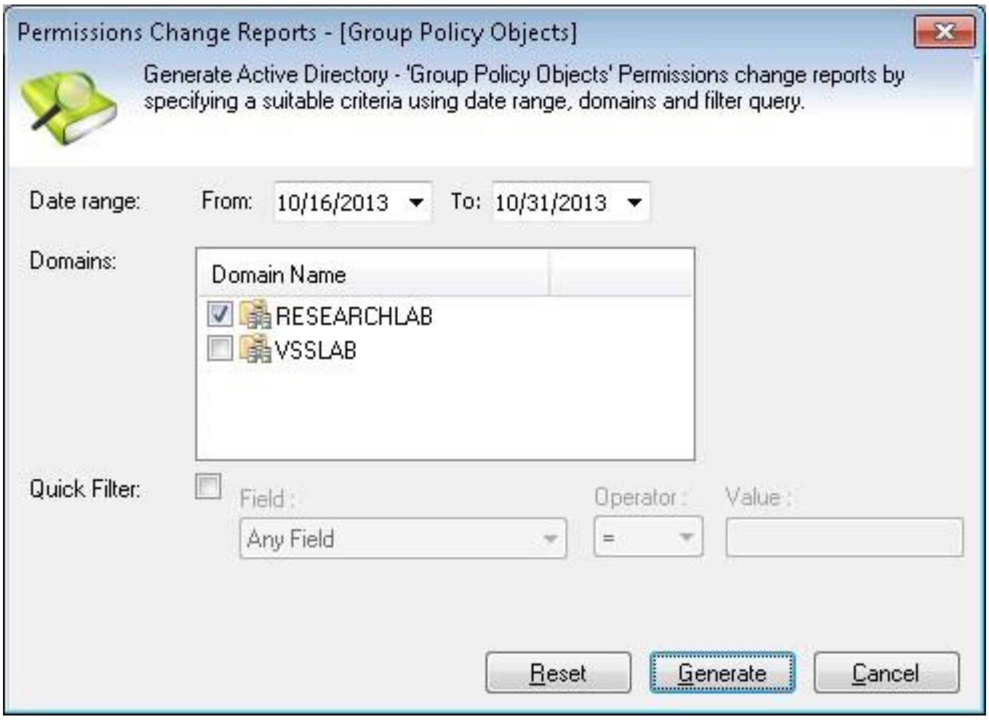
Type: Modified(Value Deleted)

3.4.7.5 How to generate Group Policy Objects Permissions change Reports?

To generate the Group Policy Objects Permissions Change Reports, perform the following steps.

1. Configure settings for 'Permissions Change Reports' as stated in Configure Events Reports.

2. To launch 'Permissions Change Reports - [Group Policy Objects]' window, click Events Reports -> Permissions Change Reports -> Group Policy Objects... menu in the toolbar. The 'Permissions Change Reports - [Group Policy Objects]' window will appear as shown below:



Permissions Change Reports - [Group Policy Objects]

Generate Active Directory - 'Group Policy Objects' Permissions change reports by specifying a suitable criteria using date range, domains and filter query.

Date range: From: 10/16/2013 To: 10/31/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

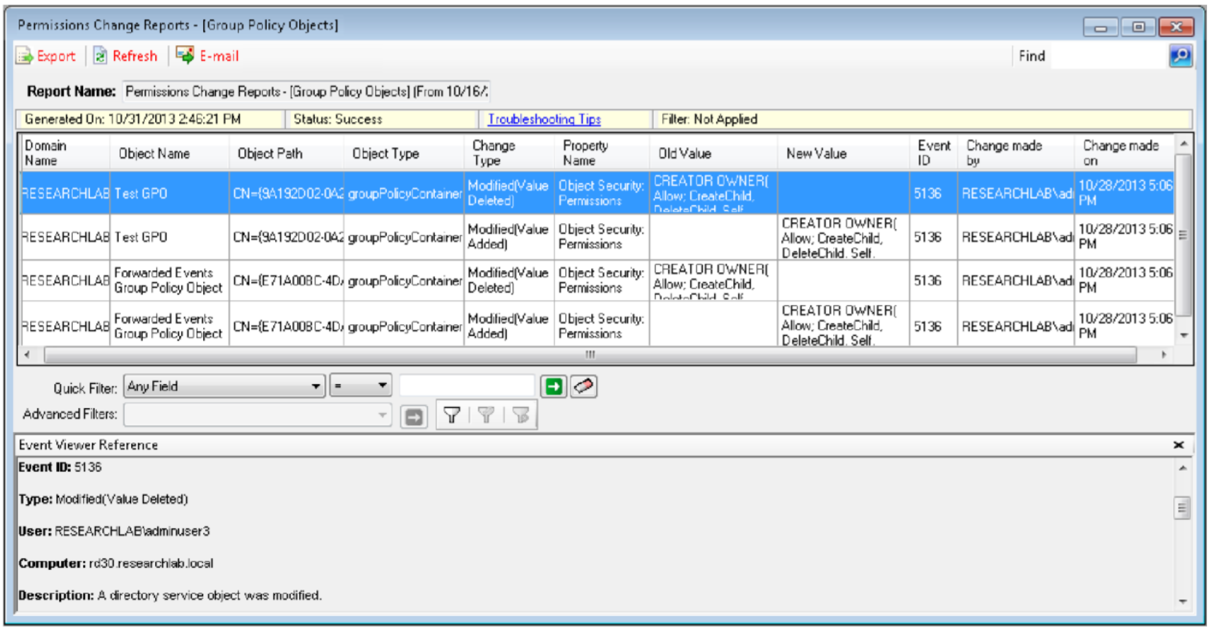
Quick Filter: □ Field : Any Field Operator : = Value :

3. Specify the Date range and a field based Filter criteria to find the Group Policy Objects Permissions change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Permissions Change Reports - [Group Policy Objects] (From 10/16/

Generated On: 10/31/2013 2:46:21 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	Test GPO	CN={9A192D02-0A2	groupPolicyContainer	Modified(Value Deleted)	Object Security: Permissions	CREATOR OWNER(Allow; CreateChild, DeleteChild, Self		5136	RESEARCHLAB\adi	10/28/2013 5:06 PM
RESEARCHLAB	Test GPO	CN={9A192D02-0A2	groupPolicyContainer	Modified(Value Added)	Object Security: Permissions		CREATOR OWNER(Allow; CreateChild, DeleteChild, Self,	5136	RESEARCHLAB\adi	10/28/2013 5:06 PM
RESEARCHLAB	Forwarded Events Group Policy Object	CN={E71A008C-4D/	groupPolicyContainer	Modified(Value Deleted)	Object Security: Permissions	CREATOR OWNER(Allow; CreateChild, DeleteChild, Self		5136	RESEARCHLAB\adi	10/28/2013 5:06 PM
RESEARCHLAB	Forwarded Events Group Policy Object	CN={E71A008C-4D/	groupPolicyContainer	Modified(Value Added)	Object Security: Permissions		CREATOR OWNER(Allow; CreateChild, DeleteChild, Self,	5136	RESEARCHLAB\adi	10/28/2013 5:06 PM

Quick Filter: Any Field | =

Advanced Filters:

Event Viewer Reference

Event ID: 5136

Type: Modified(Value Deleted)

User: RESEARCHLAB\adminuser3

Computer: rd30.researchlab.local

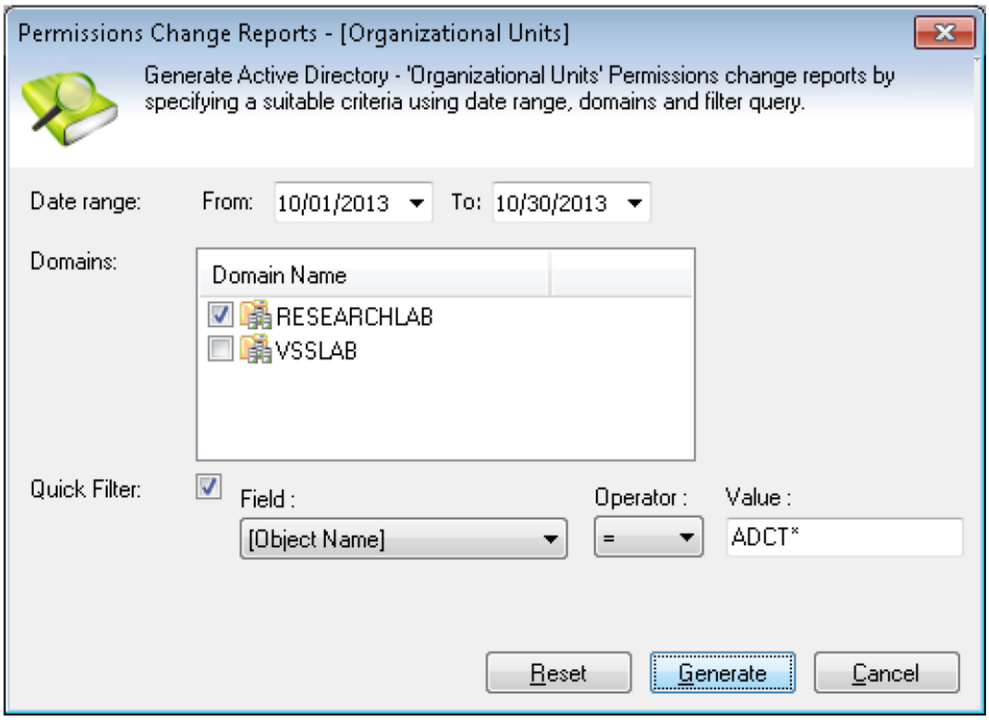
Description: A directory service object was modified.

3.4.7.6 How to generate Organizational Units Permissions change Reports?

To generate the Organizational Units Permissions Change Reports, perform the following steps.

1. Configure settings for 'Permissions Change Reports' as stated in Configure Events Reports.

2. To launch 'Permissions Change Reports - [Organizational Units]' window, click Events Reports -> Permissions Change Reports -> Organizational Units.. menu in the toolbar. The 'Permissions Change Reports - [Organizational Units]' window will appear as shown below:



Permissions Change Reports - [Organizational Units]

Generate Active Directory - 'Organizational Units' Permissions change reports by specifying a suitable criteria using date range, domains and filter query.

Date range: From: 10/01/2013 To: 10/30/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

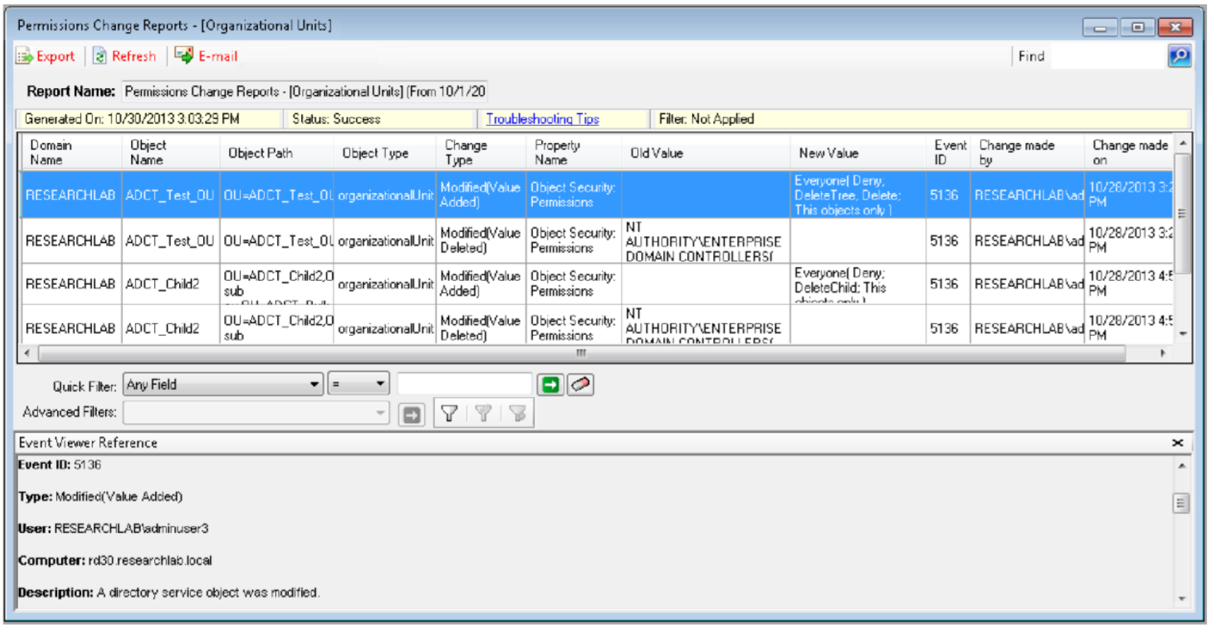
Quick Filter: ☑ Field : [Object Name] Operator : = Value : ADCT*

3. Specify the Date range and a field based Filter criteria to find the Organizational Units Permissions change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Permissions Change Reports - [Organizational Units] (From 10/1/20

Generated On: 10/30/2013 3:03:29 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	ADCT_Test_OU	OU=ADCT_Test_OU	organizationalUnit	Modified(Value Added)	Object Security: Permissions		Everyone(Deny; DeleteTree, Delete; This objects only)	5136	RESEARCHLAB\ad	10/28/2013 3:2 PM
RESEARCHLAB	ADCT_Test_OU	OU=ADCT_Test_OU	organizationalUnit	Modified(Value Deleted)	Object Security: Permissions	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS(		5136	RESEARCHLAB\ad	10/28/2013 3:2 PM
RESEARCHLAB	ADCT_Child2	OU=ADCT_Child2,O sub	organizationalUnit	Modified(Value Added)	Object Security: Permissions		Everyone(Deny; DeleteChild; This	5136	RESEARCHLAB\ad	10/28/2013 4:5 PM
RESEARCHLAB	ADCT_Child2	OU=ADCT_Child2,O sub	organizationalUnit	Modified(Value Deleted)	Object Security: Permissions	NT AUTHORITY\ENTERPRISE		5136	RESEARCHLAB\ad	10/28/2013 4:5 PM

Quick Filter: Any Field =

Advanced Filters:

Event Viewer Reference

Event ID: 5136

Type: Modified(Value Added)

User: RESEARCHLAB\adminuser3

Computer: rd30.researchlab.local

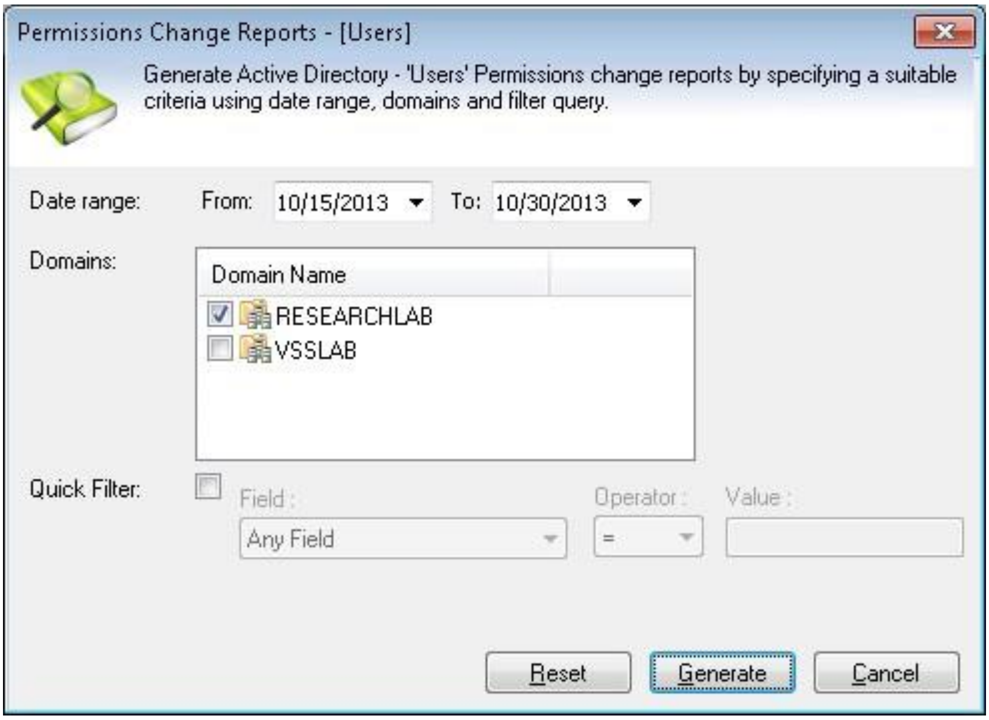
Description: A directory service object was modified.

3.4.7.7 How to generate Users Permissions Change Reports?

To generate the Users Permissions Change Reports, perform the following steps.

1. Configure settings for 'Permissions Change Reports' as stated in Configure Events Reports.

2. To launch 'Permissions Change Reports - [Users]' window, click Events Reports -> Permissions Change Reports -> Users... menu in the toolbar. The 'Permissions Change Reports - [Users]' window will appear as shown below:



Permissions Change Reports - [Users]

Generate Active Directory - 'Users' Permissions change reports by specifying a suitable criteria using date range, domains and filter query.

Date range: From: 10/15/2013 To: 10/30/2013

Domains:

Domain Name
☑ RESEARCHLAB
□ VSSLAB

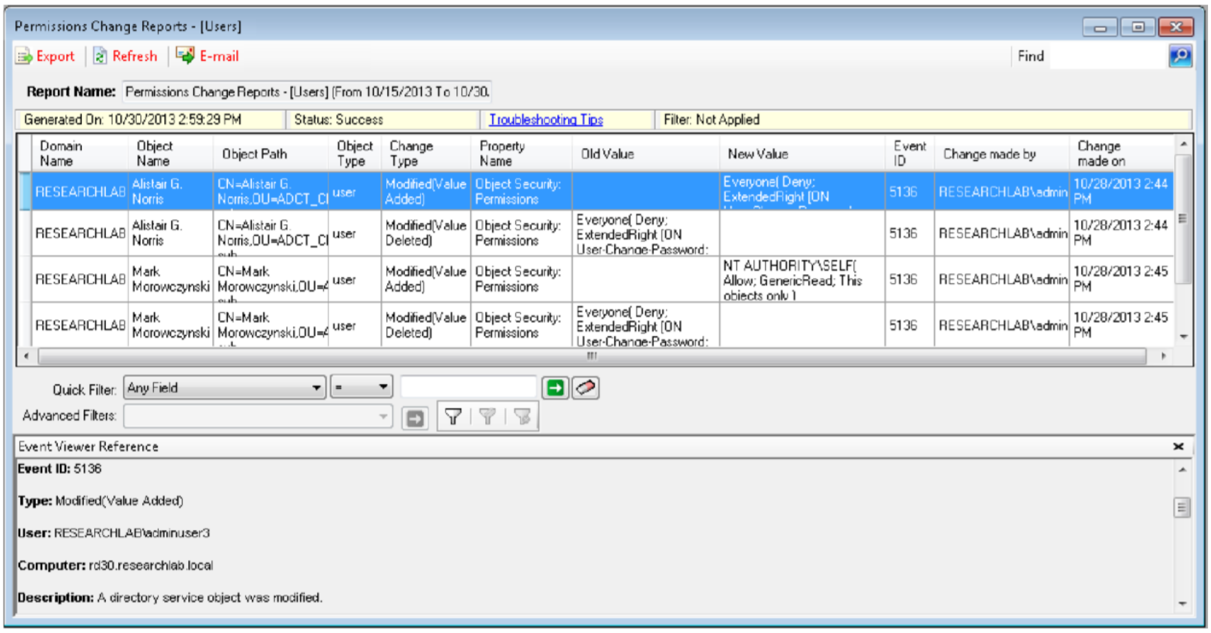
Quick Filter: □ Field : Any Field Operator : = Value :

3. Specify the Date range and a field based Filter criteria to find the Users Permissions change events in the application’s Events History database.

4. Select the desired Domains to generate your reports on.

5. Click Generate button to generate the report.

6. Once the data collection is complete, the report will be generated in a report window as shown below:



Report Name: Permissions Change Reports - [Users] (From 10/15/2013 To 10/30.

Generated On: 10/30/2013 2:59:29 PM | Status: Success | Troubleshooting Tips | Filter: Not Applied

Domain Name	Object Name	Object Path	Object Type	Change Type	Property Name	Old Value	New Value	Event ID	Change made by	Change made on
RESEARCHLAB	Alistair G. Norris	CN=Alistair G. Norris,OU=ADCT_Cl	user	Modified(Value Added)	Object Security: Permissions		Everyone(Deny; ExtendedRight [ON	5136	RESEARCHLAB\admin	10/28/2013 2:44 PM
RESEARCHLAB	Alistair G. Norris	CN=Alistair G. Norris,OU=ADCT_Cl	user	Modified(Value Deleted)	Object Security: Permissions	Everyone(Deny; ExtendedRight [ON User-Change-Password:		5136	RESEARCHLAB\admin	10/28/2013 2:44 PM
RESEARCHLAB	Mark Morowczynski	CN=Mark Morowczynski,OU=A	user	Modified(Value Added)	Object Security: Permissions		NT AUTHORITY\SELF(Allow; GenericRead; This objects only)	5136	RESEARCHLAB\admin	10/28/2013 2:45 PM
RESEARCHLAB	Mark Morowczynski	CN=Mark Morowczynski,OU=A	user	Modified(Value Deleted)	Object Security: Permissions	Everyone(Deny; ExtendedRight [ON User-Change-Password:		5136	RESEARCHLAB\admin	10/28/2013 2:45 PM

Quick Filter: Any Field =

Advanced Filters:

Event Viewer Reference

Event ID: 5136

Type: Modified(Value Added)

User: RESEARCHLAB\adminuser3

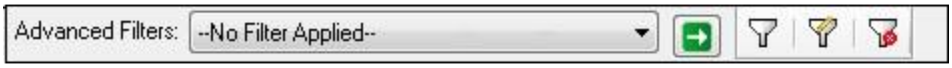
Computer: rd30.researchlab.local

Description: A directory service object was modified.

3.5 How to use Advanced Filter?

Advanced Filter tool in Events Reports allows you to filter report data based on complex filter conditions. Unlike Quick Filter, Advanced Filter gives the user the ability to create filter conditions that include one or more fields in the report and is also capable of reporting fields with empty values in the report.

The Advanced Filter tool is available below the report grid in the right pane as shown below:



Advanced Filters: --No Filter Applied--

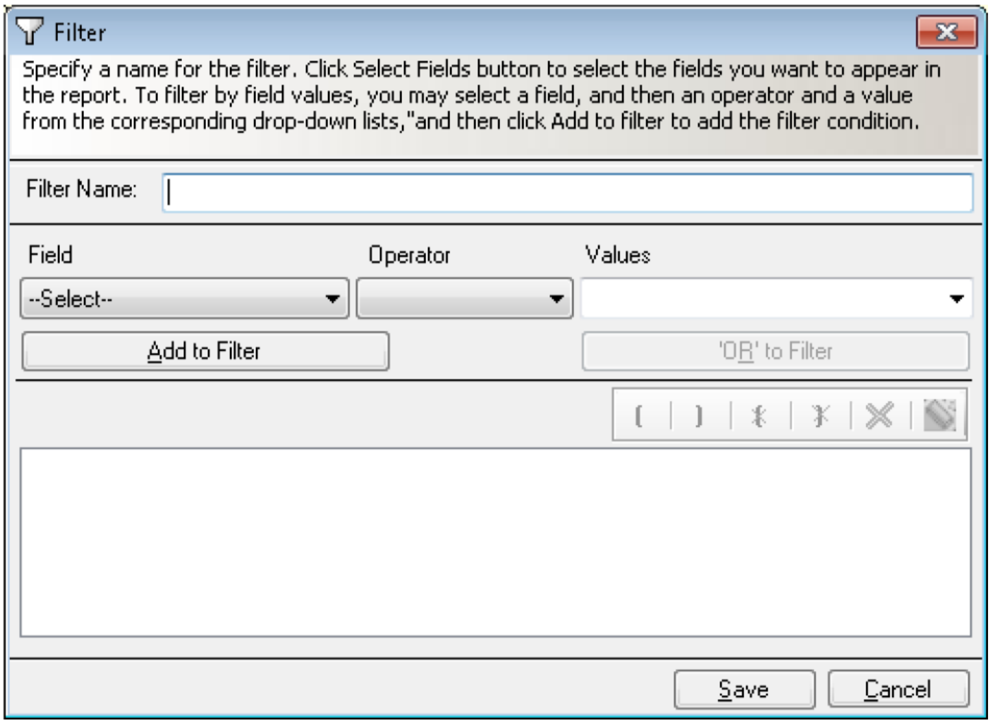
To apply a filter to the current report, select the filter from the Advanced Filters dropdown and click on ➡ button.

To remove a filter applied to the current report, select **No Filter Applied** from the Advanced Filters drop-down and click on ➡ button.

Create a new filter

Click on ▽ to create a new advanced filter for the current report.

The Filter window will appear as shown below:



Filter

Specify a name for the filter. Click Select Fields button to select the fields you want to appear in the report. To filter by field values, you may select a field, and then an operator and a value from the corresponding drop-down lists,"and then click Add to filter to add the filter condition.

Filter Name:

Field	Operator	Values
--Select--		

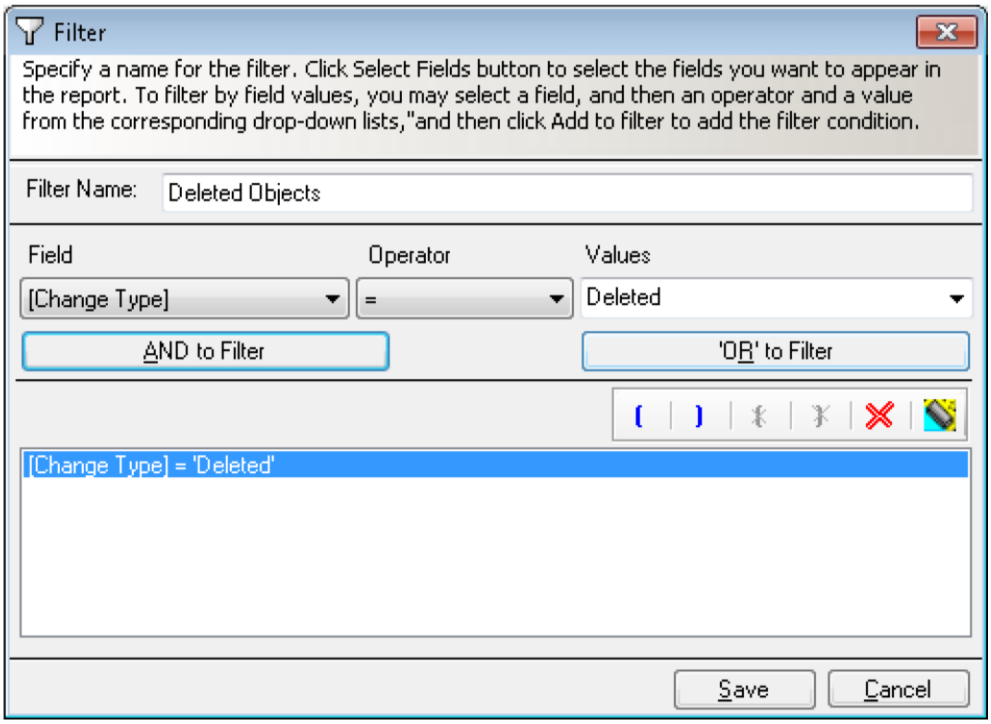
To set a filter condition, perform the following steps.

7. Specify a name for the filter.

8. Choose a field name, an operator and a possible value from the respective dropdowns.

9. Click the Add to Filter button to add the filter condition.

10. The **Add to Filter** button will change to **AND to Filter**. **OR to Filter** button will be enabled. The selected condition will be added as shown below.



Filter

Specify a name for the filter. Click Select Fields button to select the fields you want to appear in the report. To filter by field values, you may select a field, and then an operator and a value from the corresponding drop-down lists,"and then click Add to filter to add the filter condition.

Filter Name: Deleted Objects

Field: [Change Type]

Operator: =

Values: Deleted

[Change Type] = 'Deleted'

11. Click **Save** to apply the filter to the current report. Also, the filter will be saved to the filter database for future use.

The report status label above the grid, shows the filter status "**Filter**:" followed by its current status.

For a normal view, the filter status will appear as Filter: Not Applied

For a filtered view, the filter status will appear as Filter: Applied

Note:

Click to clear all the filter conditions in the list.

Use AND to Filter 'OR' to Filter and ( ) to build enhanced filter condition as shown below:

([Change Type]= 'Modified (Value Added)' AND [Property Name] = 'Telephone Number') OR ([Object Name] = 'Alex' AND [Property Name]= 'E-mail')

Use to remove the parenthesis

Use ✗ to delete a condition from the list of filter conditions. This will remove the currently selected filter condition from the list.

Edit an existing filter

To edit an existing saved filter, select the filter from the advanced filters drop-down and then click the button. The filter window will appear on the screen. You may edit the fields-list and filter conditions. Also, you can choose to save the filter in a different name, retaining the original filter, or overwrite the existing filter with the new filter conditions and fields-list.

Delete an existing filter

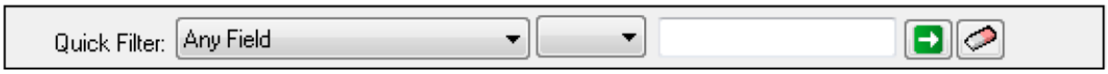
To delete an existing filter, select the filter from the advanced filters drop-down list and click the button.

However, if the filter is already applied to a report, **ADChangeTracker** clears the filter in the report and deletes the selected filter.

3.6 How to use Quick Filter?

The Quick Filter in **Events Reports** allows you to view a narrow subset of data by specifying a filter condition that could either be applied to any of the fields or to a specific field in the current report.

The Quick Filter tool is available below the report grid in the right pane as shown below:



Quick Filter: Any Field

Apply Filter

To filter report data, perform the following steps:

1. Select a field from the fields drop-down. If you want to apply the filter condition to any of the fields in the current report, select "Any Field" from the fields dropdown.

2. Select an operator from the operators drop-down, next to fields drop-down.

3. Type in a filter condition in the edit box.

Note: You can use wildcard characters such as "*" and "?" in the filter condition.

The filter condition can include regular characters as well as wildcard characters as given below:

Filter Condition	Description	Example
a*	Character starting with a	[Object Name] = a* finds object name beginning with a, for example Adminuser, Administrator.
a?	Character starting with a and maximum of two characters including a	[Object Name] = a? finds object name that has only two characters, starting with a, for example AD.
a?d*	Minimum of three characters, the first character being a, middle character may be any single character and the last character being d	[Object Name] = a?d* finds object name beginning with a, that has any single character in the middle and ending with d followed by zero or more characters.

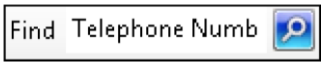
Click on ➡ to apply the filter condition.

Remove Filter

To remove the quick filter that has been applied to the current report, click the ⌫ button.

3.7 How to find data in a report?

You can use the find feature in ADChangeTracker to search for specific data in a report.

To search for data in a report, just type the characters or words you want to find in the find edit box available in the report window and click on  .

Find Telephone Numb

1. ADChangeTracker performs a case insensitive search of the specified search criteria in the report.

2. The search criteria should not be enclosed within quotation marks.

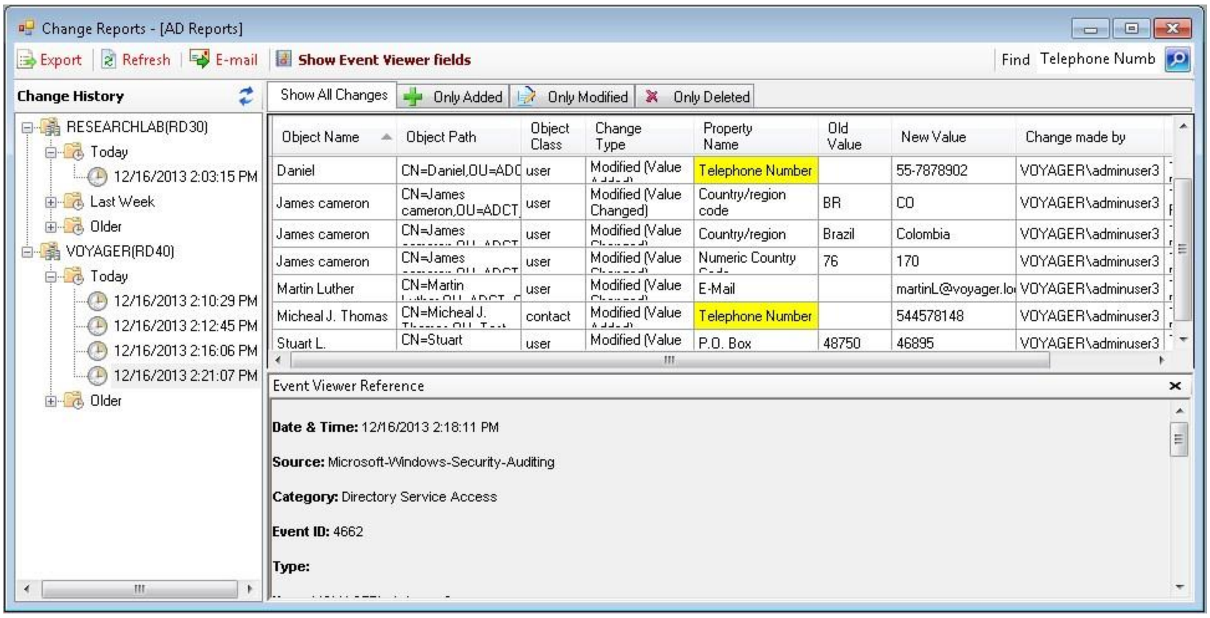
3. You can use the "*" wildcard character in the search criteria. The "*" wildcard character act as a place holder for zero or more characters. However, note that you cannot use the "?" wildcard character in the search criteria.

For instance, if you want to search for 'Domain' in a report. Type Domain, without quotations, in the edit box, and then click on Find Button.

By default, ADChangeTracker adds an asterisk as a suffix to the specified search criteria, if no wildcard character is present in it. In this case, ADChangeTracker finds a match in the report for all fields that have the text Domain followed by zero or more characters, that is, Domain, Domain Controllers, Domain Admins, etc.

For all the matches found, ADChangeTracker highlights the corresponding columns in the grid, and scrolls the grid automatically to the first occurrence.

4. ADChangeTracker finds additional occurrences of the specified search criteria instantaneously. To locate other occurrences of the same search criteria in a report you need to scroll the report grid downwards.



Object Name	Object Path	Object Class	Change Type	Property Name	Old Value	New Value	Change made by
Daniel	CN=Daniel,OU=ADC	user	Modified (Value	Telephone Number		55-7878902	VOYAGER\adminuser3
James cameron	CN=James cameron,OU=ADCT	user	Modified (Value Changed)	Country/region code	BR	CO	VOYAGER\adminuser3
James cameron	CN=James	user	Modified (Value	Country/region	Brazil	Colombia	VOYAGER\adminuser3
James cameron	CN=James	user	Modified (Value	Numeric Country	76	170	VOYAGER\adminuser3
Martin Luther	CN=Martin	user	Modified (Value	E-Mail		martinL@voyager.lo	VOYAGER\adminuser3
Micheal J. Thomas	CN=Micheal J.	contact	Modified (Value	Telephone Number		544578148	VOYAGER\adminuser3
Stuart L.	CN=Stuart	user	Modified (Value	P.O. Box	48750	46895	VOYAGER\adminuser3

Event Viewer Reference

Date & Time: 12/16/2013 2:18:11 PM

Source: Microsoft-Windows-Security-Auditing

Category: Directory Service Access

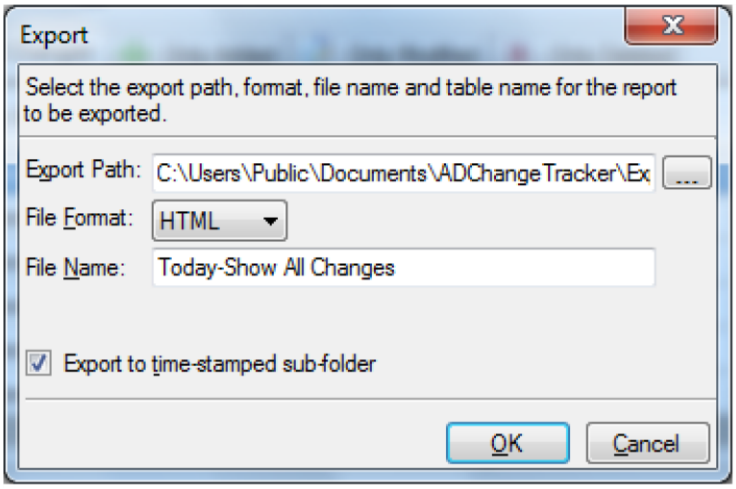
Event ID: 4662

Type:

3.8 How to Export data?

The **Export** feature helps the user to export report data generated by ADChangeTracker to a file using various formats namely HTML/CSV/XLSX.

Click on Export button in the report window or select **Export** option under **File** menu to export report data to a file in the desired format.



Export

Select the export path, format, file name and table name for the report to be exported.

Export Path: C:\Users\Public\Documents\ADChangeTracker\Ex

File Format: HTML

File Name: Today-Show All Changes

☑ Export to time-stamped sub-folder

Specify a file name to export report data to or accept the default file name. Specify the export path and select a desired file format. The path refers to the destination location where the output file generated should be stored. It can be given using the Browse button.

By default, the report will be exported to a time-stamped sub-folder in the format 'YYYYMM-DD HH.MM.SS' under the specified export path. This will be useful to avoid overwriting of existing files, if any, in the specified export path.

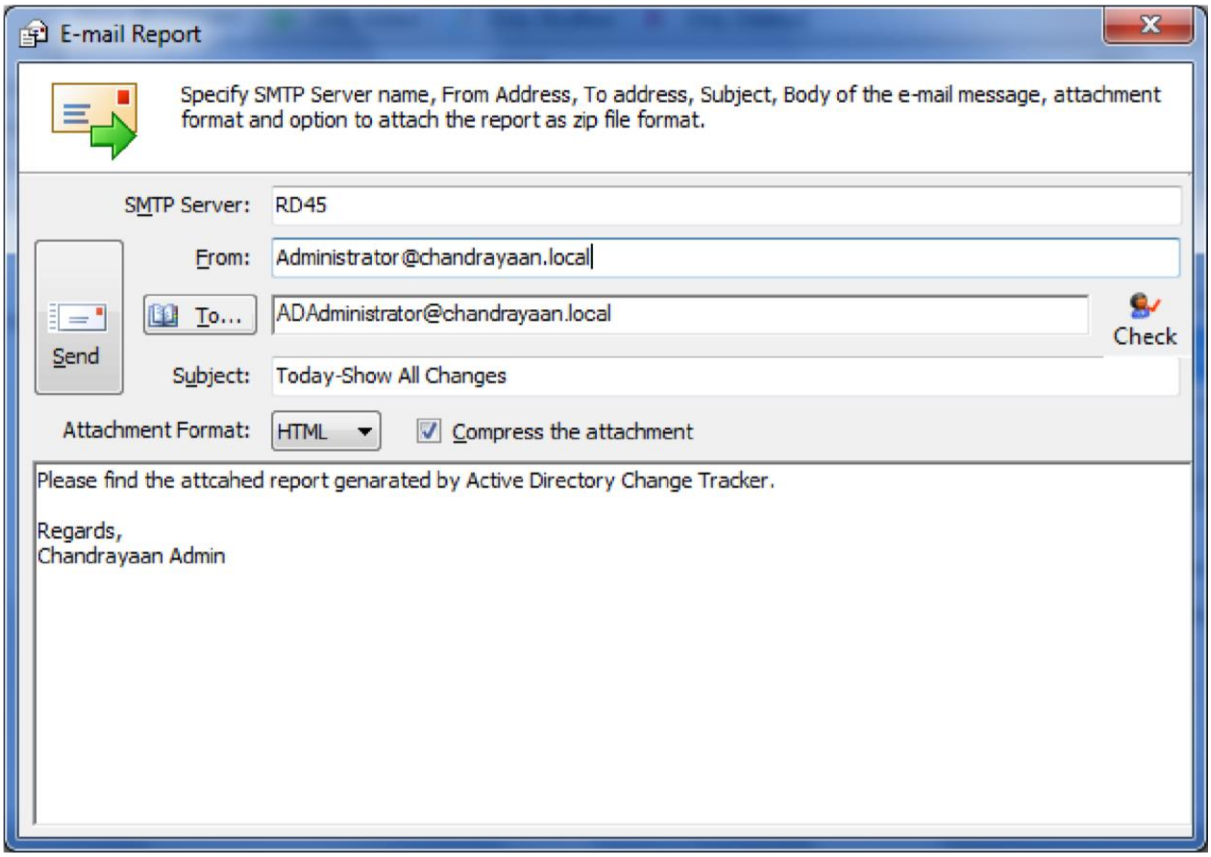
In CSV file format, the information is stored as comma separated values. For each report, a CSV file will be generated. The name of the CSV file will be the name of the report.

In HTML and XLSX file formats, the information is stored in html and xlsx files respectively. For each report, a file corresponding to the selected file format will be generated. The name of the file will be the name of the report.

3.9 How to E-mail data?

ADChangeTracker provides the option to e-mail a change report to different users. The change reports generated after tracking will be e-mailed to the specified recipients.

Click E-mail button in the toolbar to e -mail the report to e -mail recipients. E -mail dialog will be displayed as shown below:



Specify SMTP Server name, From Address, To address, Subject, Body of the e-mail message, attachment format and option to attach the report as zip file format.

SMTP Server: RD45

From: Administrator@chandrayaan.local

To... ADAdministrator@chandrayaan.local

Subject: Today-Show All Changes

Attachment Format: HTML ☑ Compress the attachment

Please find the attcahed report genarated by Active Directory Change Tracker.

Regards,
Chandrayaan Admin

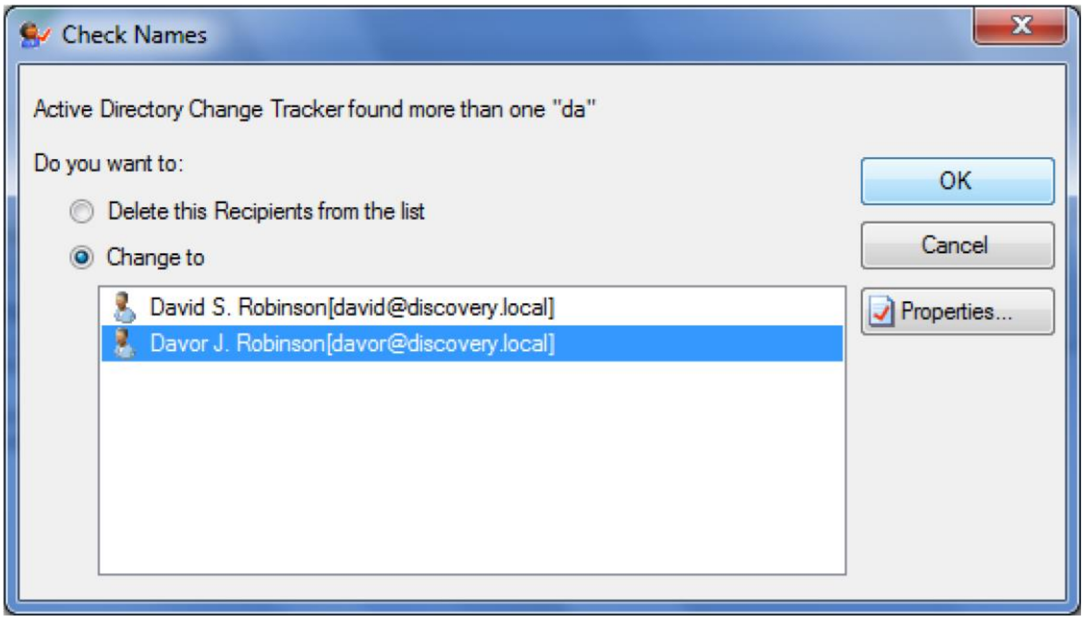
For e-mailing reports, ADChangeTracker requires the SMTP Server name, From E-mail Address, To E-mail Addresses (recipients separated by semicolon) and the report attachment format.

Specify SMTP server name, from Address, To address, mail subject, mail content, attachment format and option to compress the attachment.

Click Send button to send the report by e-mail to the selected recipients.

Check names

ADChangeTracker provides check name feature to check the existence of corresponding mail-enabled recipient object in Active Directory. To check name, click Check button. If the entered name matches with a mail object in the Active directory / its trusted domain, name entered in From address textbox will be replaced by the corresponding active directory recipient object. If there is more than one match, a dialog which contains matching Active Directory recipients will appear as shown below. You can select one or more recipients and click **OK**.



Active Directory Change Tracker found more than one "da"

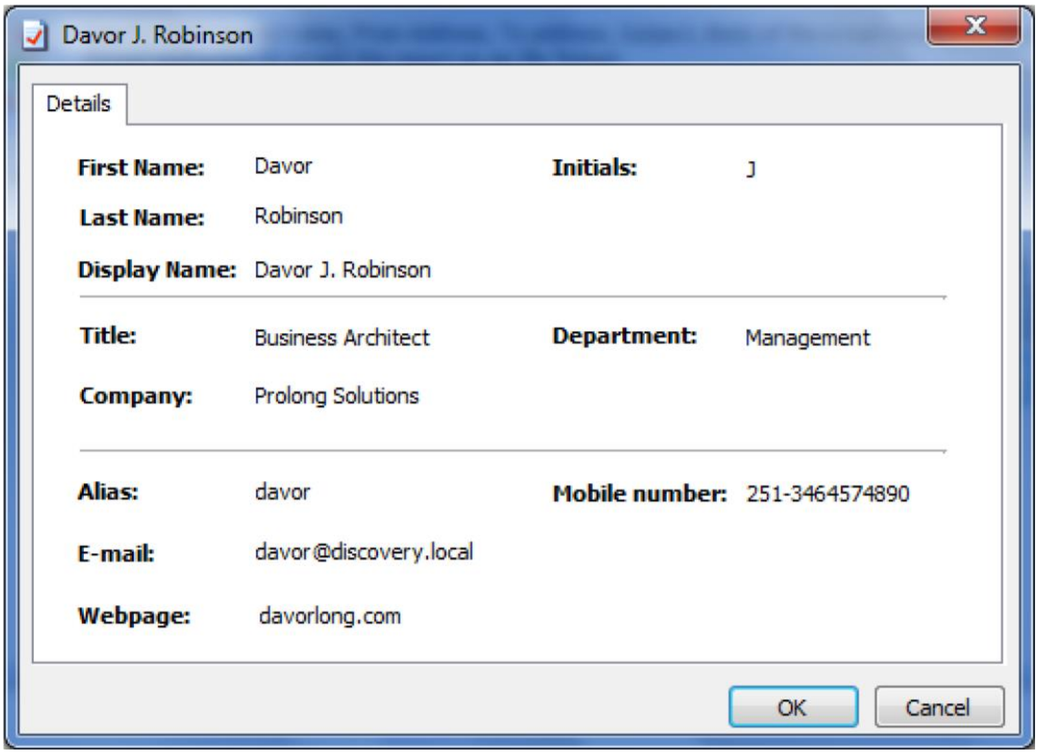
Do you want to:

○ Delete this Recipients from the list

● Change to

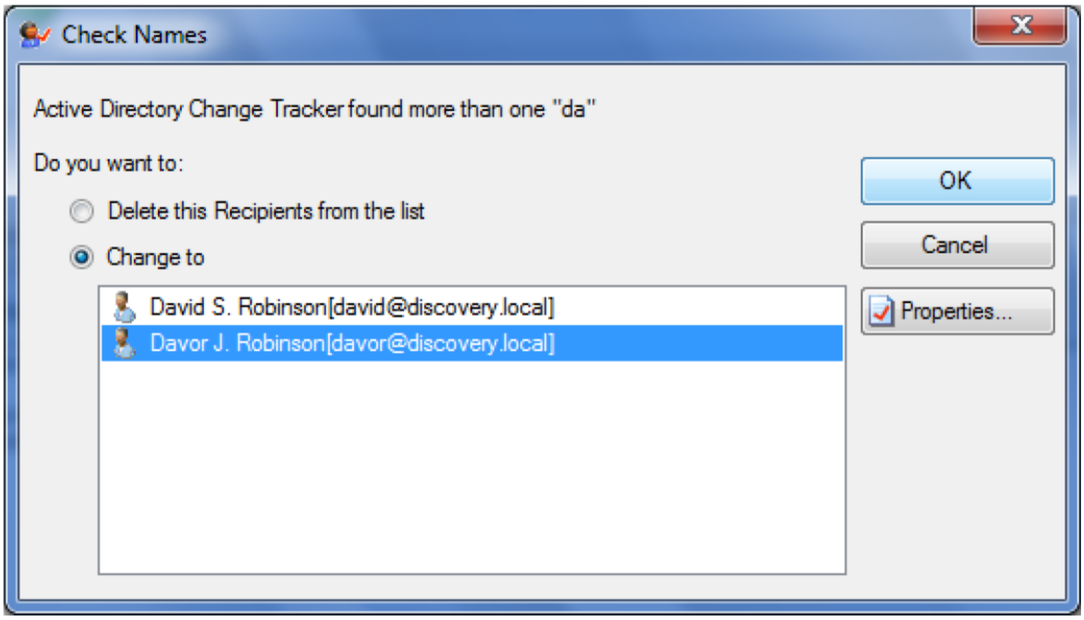
- David S. Robinson[david@discovery.local]
- Davor J. Robinson[davor@discovery.local]

To get more information about the listed recipients under Change to, select the name and then click Properties... .



First Name:	Davor	**Initials:**	J
Last Name:	Robinson		
Display Name:	Davor J. Robinson		
Title:	Business Architect	**Department:**	Management
Company:	Prolong Solutions		
Alias:	davor	**Mobile number:**	251-3464574890
E-mail:	davor@discovery.local		
Webpage:	davorlong.com		

If there is no match for the name entered by the user in Active Directory, a dialog will appear as shown below:



Active Directory Change Tracker found more than one "da"

Do you want to:

○ Delete this Recipients from the list

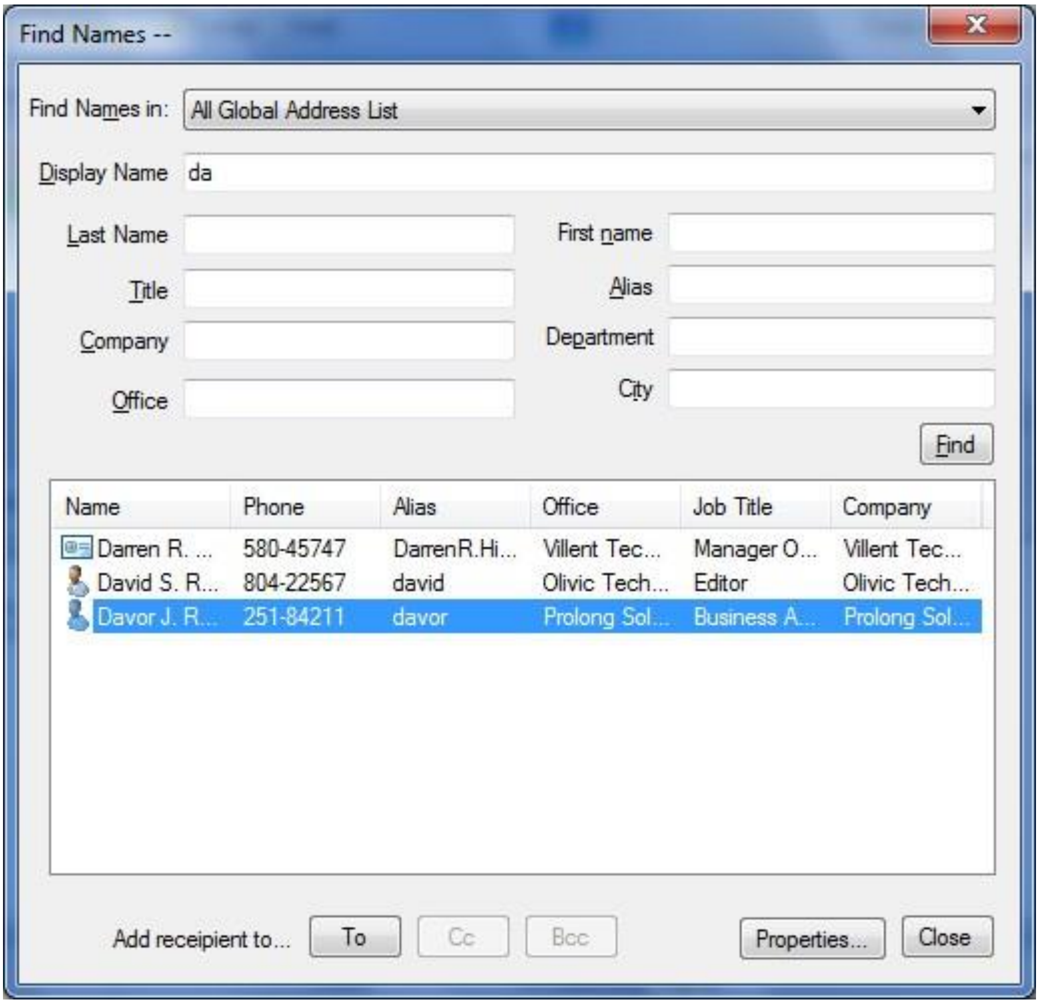
● Change to

David S. Robinson[david@discovery.local]
Davor J. Robinson[davor@discovery.local]

Select Delete option in the above dialog to remove the recipient name from To address text box. Click Cancel button to close this dialog and the unresolved recipient(s) will appear in red color.

Address Book

ADChangeTracker provides Address Book feature to search for any mail enabled recipient object (say, person, distribution list, contact, public folder) you want to send a message to. Click To... button and then use the **Find Names** dialog box to search for the recipient object you want to send a message to. (Note that you can't use the **Find Names** dialog box to search for distribution lists in your Contacts folder.) Select the object's name in the list and then click **Add recipient to**...To.



Find Names in: All Global Address List

Display Name da

Name	Phone	Alias	Office	Job Title	Company
Darren R. ...	580-45747	DarrenR.Hi...	Villent Tec...	Manager O...	Villent Tec...
David S. R...	804-22567	david	Olivic Tech...	Editor	Olivic Tech...
Davor J. R...	251-84211	davor	Prolong Sol...	Business A...	Prolong Sol...

To get more informa tion about one of the names in the list, such as department or phone number, select the name, and then click Properties... .

4 User Profiles

ADChangeTracker creates a user profile in **Windows Stored User Names and Passwords** applet, in order to store the SQL and Directory Server user context for report generation.

The stored user profile will be useful for generating reports using ADChangeTracker under the following scenarios:

a. Using an SQL Server having a dedicated SQL user account for report generation using ADChangeTracker (highly recommended)

b. Using an SQL Server where SQL authentication mode is enabled

c. Using an alternate user account to connect to the Directory Server to retrieve AD information

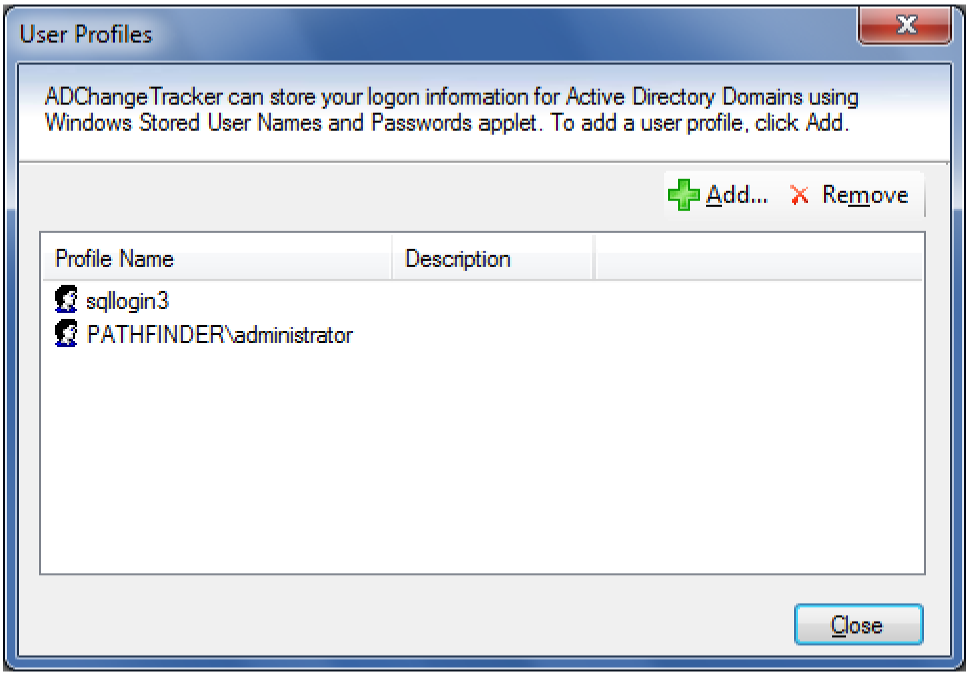
The stored user profile persists for all subsequent logon sessions on the same computer where ADChangeTracker is installed. The stored user profiles are visible to the application under other logon sessions on the same computer.

The stored user profile created by ADChangeTracker is restricted to the Windows User Profile context. If the Windows User Profile is maintained locally, ADChangeTracker stored user profile is accessible only by the same user in the same computer. If the user who creates ADChangeTracker stored user profile, has a Roaming user account in the enterprise, the ADChangeTracker stored user profile can be accessed by the same user in any computer in the Windows enterprise.

The stored user profile is a generic credential of **Windows Stored User Names and Passwords** applet and can be used by ADChangeTracker application only. The credential information is stored securely in an *256 bit encrypted format* in **Windows Stored User Names and Passwords** applet.

The stored user profile corresponding to the SQL user account will be used by ADChangeTracker application in order to connect to the SQL Server, if SQL authentication is enabled in ADChangeTracker SQL settings.

Using the User Profiles dialog shown below, new profile can be created and available profiles can be removed from the profiles list.

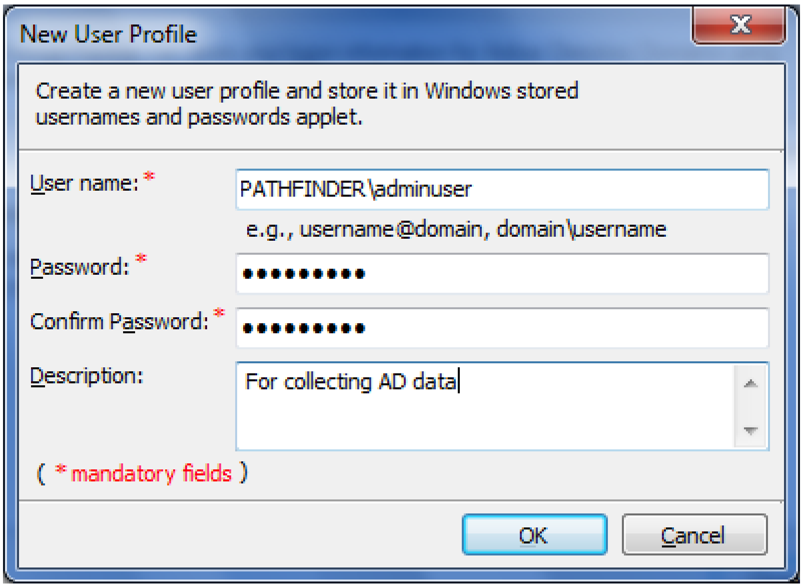


User Profiles

ADChangeTracker can store your logon information for Active Directory Domains using Windows Stored User Names and Passwords applet. To add a user profile, click Add.

Profile Name	Description
sqllogin3	
PATHFINDER\administrator	

Click New button to add a new profile and a dialog will appear as shown below:



New User Profile

Create a new user profile and store it in Windows stored usernames and passwords applet.

User name: * PATHFINDER\adminuser

e.g., username@domain, domain\username

Password: * ●●●●●●●●●

Confirm Password: * ●●●●●●●●●

Description: For collecting AD data

(* mandatory fields)

Click Remove button in the User Profiles dialog to remove available profiles.

5 References

Frequently asked questions
How to uninstall ADChangeTracker
Technical Support

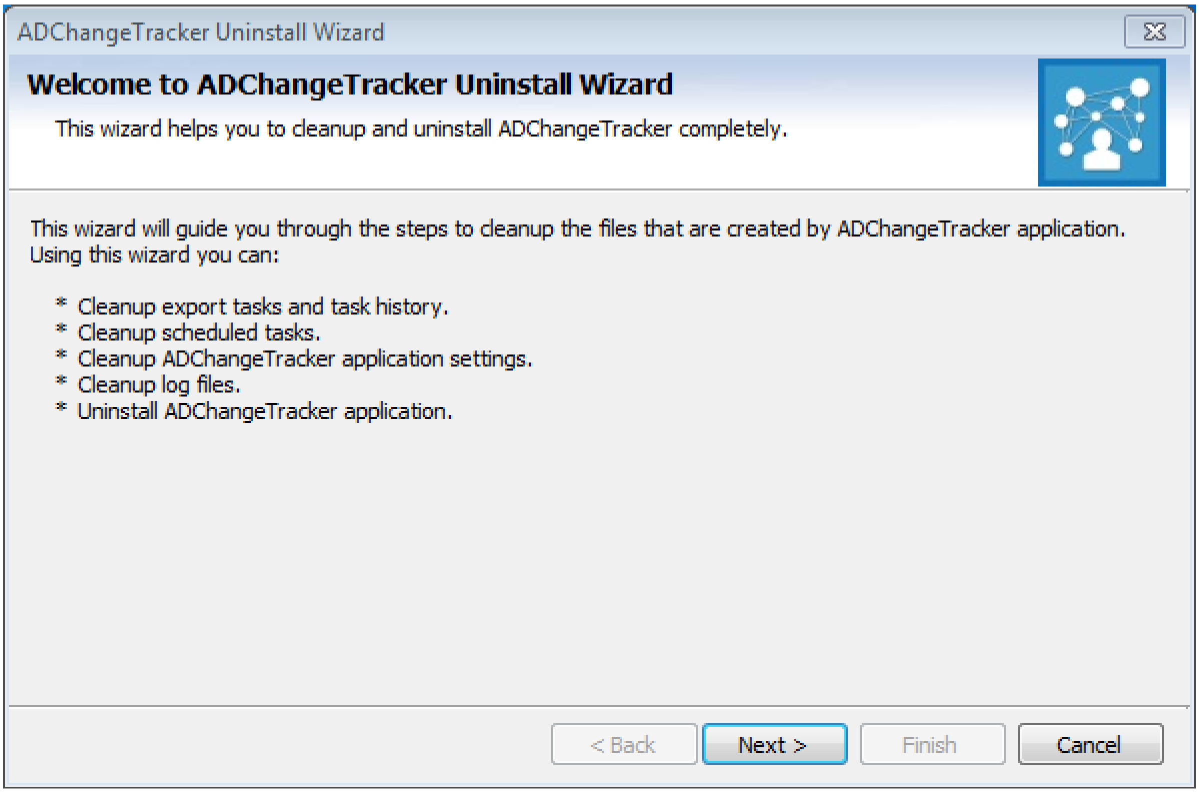
5.1 How to Uninstall ADChange Tracker?

When you *uninstall ADChangeTracker* through **Control Panel - Add / Remove Programs** applet, *Windows Installer program* will remove only the application files from your computer. But, the application related files created by ADChangeTracker remain in the computer. In order to remove ADChangeTracker worker files completely, the *uninstall wizard* provides a set of *cleanup options* to perform the cleanup operation based upon your selection.

Use this wizard to cleanup the files that are created by ADChangeTracker application selectively and *uninstall ADChangeTracker completely* from the computer.

1) Launch the *Uninstall wizard* by clicking **Start -> Programs -> Active Directory Change Tracker -> Uninstall ADChangeTracker.**

2) The **ADChangeTracker Uninstall Wizard** dialog will be shown as below:



Welcome to ADChangeTracker Uninstall Wizard

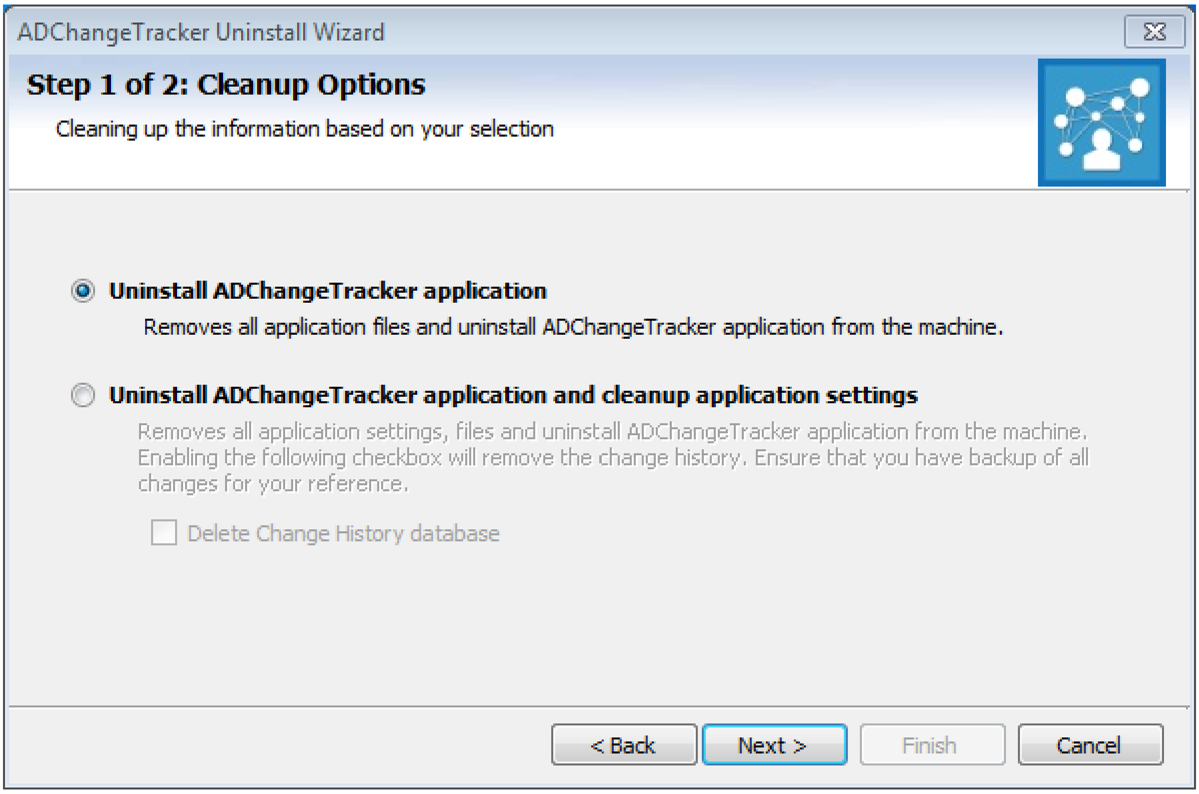
This wizard helps you to cleanup and uninstall ADChangeTracker completely.

This wizard will guide you through the steps to cleanup the files that are created by ADChangeTracker application.
Using this wizard you can:

* Cleanup export tasks and task history.
* Cleanup scheduled tasks.
* Cleanup ADChangeTracker application settings.
* Cleanup log files.
* Uninstall ADChangeTracker application.

Click **Next** to Proceed.

3) ***Select*** required ***cleanup options*** as shown below:


ADChangeTracker Uninstall Wizard

Step 1 of 2: Cleanup Options

Cleaning up the information based on your selection

● Uninstall ADChangeTracker application

Removes all application files and uninstall ADChangeTracker application from the machine.

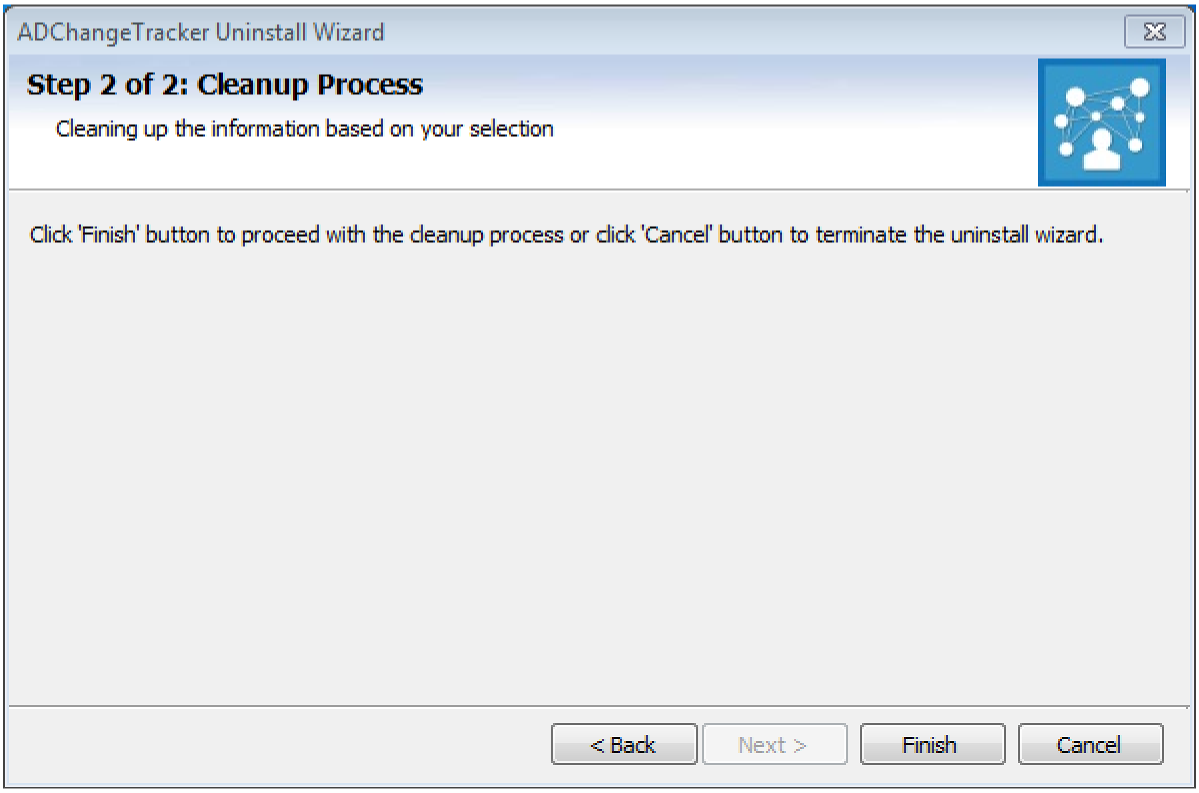
○ Uninstall ADChangeTracker application and cleanup application settings

Removes all application settings, files and uninstall ADChangeTracker application from the machine. Enabling the following checkbox will remove the change history. Ensure that you have backup of all changes for your reference.

□ Delete Change History database

Click **Next** to Proceed.

4) ***Confirm*** the ***cleanup and/or uninstall*** process.


ADChangeTracker Uninstall Wizard

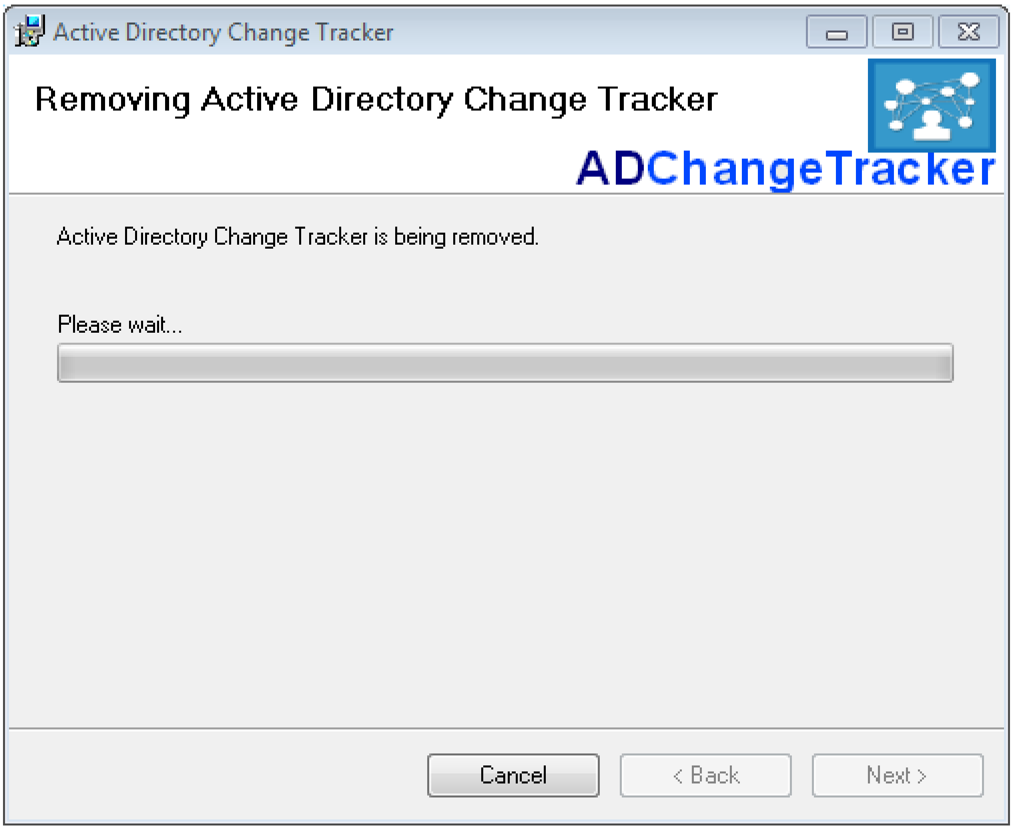
Step 2 of 2: Cleanup Process

Cleaning up the information based on your selection

Click 'Finish' button to proceed with the cleanup process or click 'Cancel' button to terminate the uninstall wizard.

CHAPTER-5- References

Click **Finish** to run cleanup and/or uninstall process. Click **Cancel** to close the wizard.



Removing Active Directory Change Tracker

Active Directory Change Tracker is being removed.

Please wait...

1) Once the file cleanup process is *complete*, the *uninstall wizard* will automatically run *Windows Installer* program to *remove* ADChangeTracker *application* from the computer.

5.2 Technical Support

If and when a problem arises, please forward the following information to support@vyapin.com to revert back to you with a solution.

Error log file - e.g., <Application Data Folder>\ADChangeTracker\ADChangeTrackerErrorLog.log

The *<Application Data Folder>* is the common location where ADChangeTracker settings will be stored in the computer running ADChangeTracker application. The *<Application Data Folder>* can be found from the **Help -> About** screen. The default path of *<Application Data Folder>* is as follows:

a) Windows XP, Windows 2003 - C:\Documents and Settings\All Users\Documents

b) Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2 - C:\Users\Public\Documents

6 Index