

Setup ADchangeTracker instructions

Installation and configuration of ADchangeTracker service.

Please see [Active-Directory-change-tracking](#) for more information.

Table of Contents

1	Configure Event Logging in Active Directory	1
2	Create a service user in Active Directory	2
3	Grant service user permission to read Security Log on all DC's	3
4	Create security group for AD reports	3
5	Create a database in SQL server	3
6	Create logins and grant permissions in SQL server	4
7	Install ADchangeTracker service on all writable DC's	4
8	Install and configure reports in SSRS	5

In the downloaded ZIP file you will find the following files:

Filename	What is it	To Do
Setup ADchangeTracker instructions.PDF	This document	Read it
Active Directory change auditing screenshots.PDF	AD event logging help	
Setup.exe	The ADchangeTracker service	Run on Domain Controllers
CreateAD_DWdatabase.sql	Create DB T-SQL script	Run on SQL server
CreateLogins.sql	Create logins T-SQL script	Run on SQL server
AD_Events.rdl	SSRS report	Upload to SSRS server
EventXml.rdl	SSRS report	Upload to SSRS server

1 Configure Event Logging in Active Directory

You will need Domain Admin permissions to perform this task.

This is by far the most time consuming task – also the most technical.

Use **Group Policy Management** tool and **Active Directory Users and Computers** tool to perform the tasks required in this step.

Note – you can continue and complete the remaining steps of the ADchangeTracker setup process even if you have not successfully completed this one. But you will not see much data flowing into the SQL DB unless AD change events are generated into the Security Log.

This web page provides very good information on how to do this:

[How to enable Active Directory Change Events](#)

Please see also the included document “Active Directory change auditing screenshots.PDF”.

After you have completed this step – you should verify that AD change events are generated when an object in AD is changed. See this reference: [Active Directory Change and Security Event IDs](#)

Here are a few other websites for reference:

[Who Moved the AD Cheese?](#)

[AD DS Auditing Step-by-Step Guide](#)

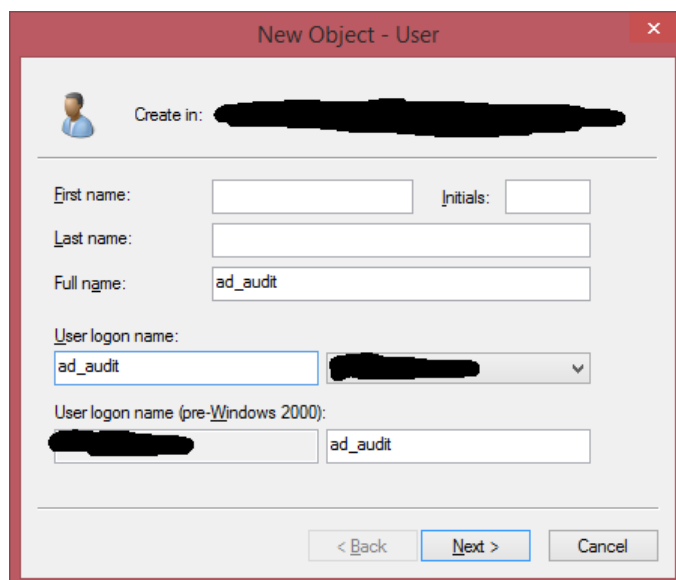
[Active Directory Services Audit - Document references](#)

2 Create a service user in Active Directory

You will need Domain Admin permissions to perform this task.

Use **Active Directory Users and Computers** tool to perform the task required in this step.

Create a user named “**ad_audit**” in an OU where you normally keep service users (you can change the name of course).



The screenshot shows the 'New Object - User' dialog box in the Active Directory Users and Computers tool. The dialog has a title bar with a close button. Inside, there's a 'Create in:' field with a dropdown menu showing a specific OU. Below this are several input fields: 'First name:', 'Initials:', 'Last name:', 'Full name:' (containing 'ad_audit'), 'User logon name:' (containing 'ad_audit'), and 'User logon name (pre-Windows 2000):' (containing 'ad_audit'). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

This user will run the **ADchangeTracker** service on all writable domain controllers. The user needs permissions to read the **Security Log** on the domain controllers (Step 3) and will also need permissions to execute stored procedures in the **AD_DW** SQL database (Step 6).

3 Grant the service user permission to read Security Log on all DC's

You will need Domain Admin permissions to perform this task.

Use **Active Directory Users and Computers** tool to perform the task required in this step.

Click on "**Builtin**" OU, double click "**Event Log Readers**" group. Add "**ad_audit**" user to the group.

This will grant the user permission to read the **Security Log** on all Domain Controllers.

4 Create security group for SSRS reports

You will need Domain Admin permissions to perform this task.

Use **Active Directory Users and Computers** tool to perform the task required in this step.

Create a security group named "**SG-ADreports**" in an OU where you normally keep such groups. Add all the users you want to have access to the reports (you can change the group name of course).

Note – the users you added to the group will need to log out and then in again on their workstations before group membership is updated.

This security group will be used both in SQL server and in SQL Server Reporting Services.

5 Create a database in SQL server

You will need SysAdmin permissions in SQL server to perform this task.

Use **SQL Management Studio** tool to perform the task required in this step.

Connect to the SQL server where the database will reside, open the included **CreateAD_DWdatabase.sql** file and run it.

This T-SQL script will create the **AD_DW** database, tables, indices, views and stored procedures.

6 Create logins and grant permissions in SQL server

You will need SysAdmin permissions in SQL server to perform this task.

Use **SQL Mangement Studio** tool to perform the task required in this step.

Connect to the SQL server where the **AD_DW** database is found, open the included **CreateLogins.sql** file.

Now do a find/replace on “DOMAIN” replace with your domain name in the script.

Now run the script.

This T-SQL script will grant read, execute permissions to the **SG-ADreports** security group and execute to the **ad_audit** user on the **AD_DW** database.

7 Install ADchangeTracker service on all writable DC's

You will need Domain Admin permissions to perform this task.

Do the following on **all writable domain controllers** in your domain.

- Log on to a domain controller.
- Run the included **Setup.exe**.

After setup completes you will find a new service “Active Directory change tracker” in the list of services. This service is not running yet, you need to configure a few things before it can run.

- Run **Notepad** as Administrator.
- Open the **C:\Program Files (x86)\ADchangeTracker\ADchangeTracker.cfg** file.
- Edit the “*# SqlConnString etc*” line, remove the “# ” (hashtag space) from the beginning of the line and change ‘*SQLserverName*’ to the name of the SQL server where the **AD_DW** database is found.
- You don’t need to change the other settings in the file.
- Save the file and close Notepad.
- Open **Services** tool.
- Right click on the **Active Directory change tracker** service, select **Properties**.
- Click on **Log On** tab.
- Select **This account**, click **Browse** button, type “**ad_audit**” in the textbox. Click **Locations** button, select “**Entire Directory**” and click **OK** button. Click **Check Names** button and if no error; click **OK** button.
- Type the password for user **ad_audit** in the textboxes for password and click **OK** button.
- Click on **General** tab.
- Change **Startup type** to **Automatic**.
- Click **Apply** button.
- Click **Start** button.
- Click **OK** button.

Open **File Explorer** and go to **C:\ProgramData\ADchangeTracker** (note – **ProgramData** is a hidden folder).

Open the log file in **Notepad** that was created when the service started. Check for any errors.

Log files are named like this: **ADchangeTracker_YYYY-MM-DD_HH-MM-SS.log**

8 Install and configure reports in SSRS

You will need System Administrator permissions on SSRS to perform this task.

Open **Internet Explorer** and browse to the **Home** page of the **SQL Server Reporting Services** server.

Grant the SG-ADreports security group Browser permission on the Home folder.

The image shows a sequence of three screenshots from the SQL Server Reporting Services (SSRS) web interface. The first screenshot shows the 'Home' page with a toolbar containing 'New Folder', 'New Data Source', 'Report Builder', 'Folder Settings', and 'Upload File'. A red arrow points to the 'Folder Settings' button. The second screenshot shows the 'New Role Assignment' dialog box, with a red arrow pointing to the 'New Role Assignment' button. The third screenshot shows the 'New Role Assignment' dialog box with the 'Group or user name' field set to 'SG-ADreports' and the 'Browser' role selected. A red arrow points to the 'Browser' role checkbox. Below the role list are 'OK' and 'Cancel' buttons.

SQL Server Reporting Services - [REDACTED]
Home

New Folder | New Data Source | Report Builder | Folder Settings | Upload File

SQL Server Reporting Services - [REDACTED]
Home

Delete | New Role Assignment

Home

SQL Server Reporting Services - [REDACTED]
New Role Assignment

Use this page to define role-based security for Home.

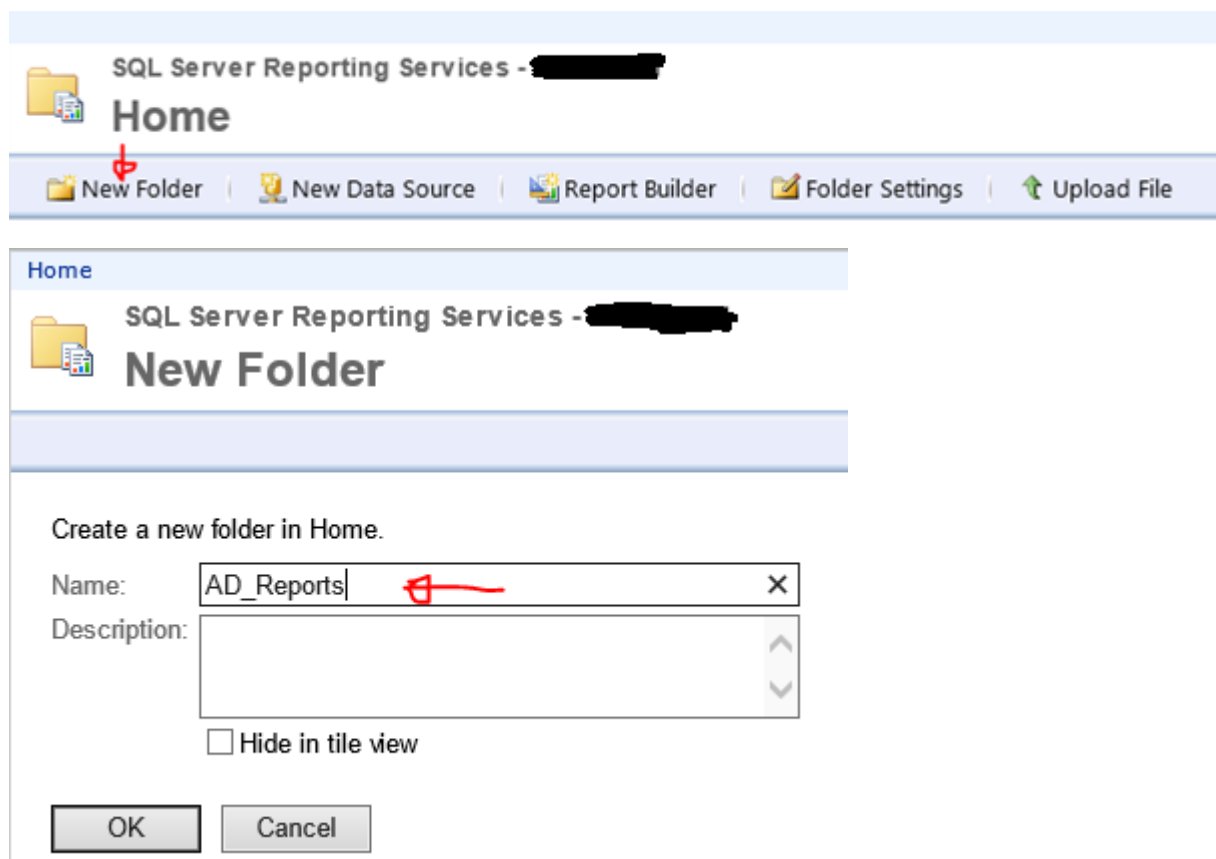
Group or user name: [REDACTED]:SG-ADreports

Select one or more roles to assign to the group or user.

<input type="checkbox"/>	Role ↓	Description
<input checked="" type="checkbox"/>	Browser	May view folders, reports and
<input type="checkbox"/>	ConfigMgr Report Administrators	May perform all tasks related
<input type="checkbox"/>	ConfigMgr Report Users	May run reports and create re
<input type="checkbox"/>	Content Manager	May manage content in the F
<input type="checkbox"/>	My Reports	May publish reports and linke
<input type="checkbox"/>	Publisher	May publish reports and linke
<input type="checkbox"/>	Report Builder	May view report definitions.

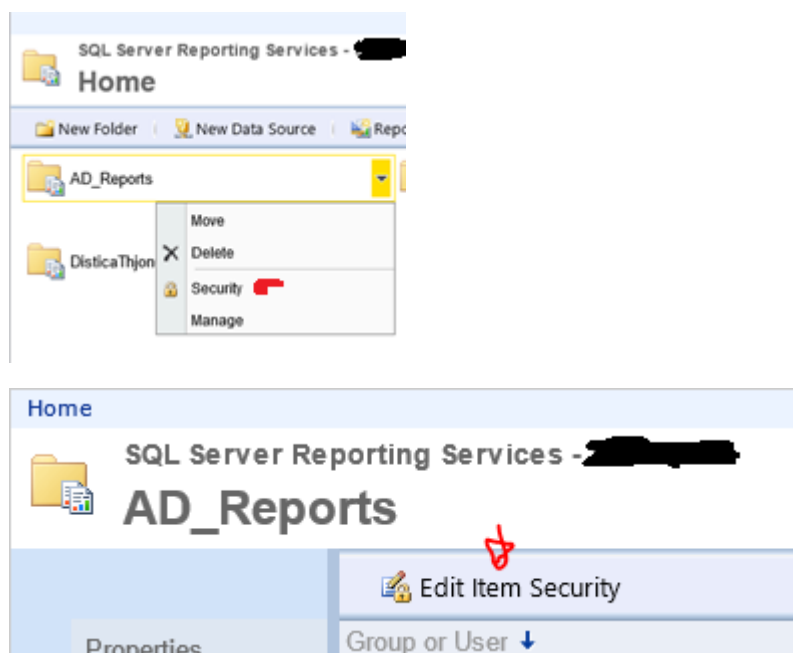
OK Cancel

Create a new folder "AD_Reports" (you can change the name of course).



The screenshot shows the 'Home' page of SQL Server Reporting Services. The breadcrumb trail is 'Home'. The main heading is 'SQL Server Reporting Services - [redacted]'. Below the heading, there is a toolbar with buttons: 'New Folder', 'New Data Source', 'Report Builder', 'Folder Settings', and 'Upload File'. The 'New Folder' button is highlighted with a red arrow. Below the toolbar, the page title is 'Home'. The main content area shows 'SQL Server Reporting Services - [redacted]' and 'New Folder'. A dialog box is open with the title 'Create a new folder in Home.' The 'Name' field contains 'AD_Reports' and is highlighted with a red arrow. The 'Description' field is empty. There is a checkbox labeled 'Hide in tile view' which is unchecked. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Grant SG-ADreports security group Browser permission on the folder.



The screenshot shows the 'AD_Reports' folder in SQL Server Reporting Services. The breadcrumb trail is 'Home'. The main heading is 'SQL Server Reporting Services - [redacted]'. Below the heading, there is a toolbar with buttons: 'New Folder', 'New Data Source', and 'Report Builder'. The 'AD_Reports' folder is selected, and a context menu is open with options: 'Move', 'Delete', 'Security', and 'Manage'. The 'Security' option is highlighted with a red arrow. Below the context menu, the page title is 'Home'. The main content area shows 'SQL Server Reporting Services - [redacted]' and 'AD_Reports'. At the bottom, there is a 'Properties' tab and a 'Group or User' dropdown menu. The 'Edit Item Security' button is highlighted with a red arrow.

Home

SQL Server Reporting Services - [REDACTED]

AD_Reports

Delete | New Role Assignment | Revert to Parent Security

Properties ☐ Group or User Role(s)

Home

SQL Server Reporting Services - [REDACTED]

New Role Assignment

Use this page to define role-based security for AD_Reports.

Group or user name: [REDACTED]SG-ADreports

Select one or more roles to assign to the group or user.

<input type="checkbox"/>	Role	Description
<input checked="" type="checkbox"/>	Browser	May view folders, reports and report definitions
<input type="checkbox"/>	ConfigMgr Report Administrators	May perform all tasks relating to reports and report definitions
<input type="checkbox"/>	ConfigMgr Report Users	May run reports and create report definitions
<input type="checkbox"/>	Content Manager	May manage content in the report server
<input type="checkbox"/>	My Reports	May publish reports and list reports
<input type="checkbox"/>	Publisher	May publish reports and list reports
<input type="checkbox"/>	Report Builder	May view report definitions

Upload the supplied two report files - AD_Events.rdl and EventXml.rdl.

Home

SQL Server Reporting Services - [REDACTED]

AD_Reports

New Folder | New Data Source | Report Builder | Folder Settings | Upload File

Home > AD_Reports

SQL Server Reporting Services - [REDACTED]

Upload File

Upload a report (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc)

File to upload: E:\Temp\AD_Events.rdl 

Name: AD_Events

☐ Overwrite item if it exists

Home > AD_Reports

SQL Server Reporting Services - [REDACTED]

Upload File

Upload a report (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc)

File to upload: E:\Temp\EventXml.rdl 

Name: EventXml

☐ Overwrite item if it exists

Set the EventXml report as hidden (because it's a subreport).


Home

SQL Server Reporting Services - [REDACTED]

AD_Reports

X Delete | Move | New Folder | New Data Source

Type	Name
<input type="checkbox"/>	AD_Events
<input type="checkbox"/>	EventXml



- Move
- Delete
- Subscribe...
- Create Linked Report...
- View Report History
- Security
- Manage
- Download...
- Edit in Report Builder



EventXml

✕ Delete

📁 Move

🔗 Create Linked Report

⬇️ Download

Properties

Parameters

Data Sources

Subscriptions

Processing Options

Cache Refresh Options

Report History

Snapshot Options

Security

Modified Date: 21.6.2015 12:51

Modified By: [REDACTED]

Creation Date: 3.6.2015 15:47

Created By: [REDACTED]

Size: 13 KB

Properties

Name: EventXml

Description:

☒ Hide in tile view



Apply

Create a linked report when you want to use different security or parameters

Change the connection string for the reports – set the name of your SQL server.

Home > AD_Reports Home | My

SQL Server Reporting Services - [REDACTED]

AD_Events

- Properties
- Parameters
- Data Sources**
- Subscriptions
- Processing Options
- Cache Refresh Options
- Report History
- Snapshot Options
- Security


Data Source1

☐ A shared data source

Select a shared data source

☒ A custom data source

Data source type:

Connection string: 

Connect using:

☐ Credentials supplied by the user running the report

Display the following text to prompt user for a user name and password:

☐ Use as Windows credentials when connecting to the data source

☐ Credentials stored securely in the report server

User name:

Password:

☐ Use as Windows credentials when connecting to the data source

☐ Impersonate the authenticated user after a connection has been made to the data source

☒ Windows integrated security

☐ Credentials are not required

[Properties](#)[Parameters](#)**[Data Sources](#)**[Subscriptions](#)[Processing Options](#)[Cache Refresh Options](#)[Report History](#)[Snapshot Options](#)[Security](#)**Data Source1**☐ A shared data source

Select a shared data source

[Browse](#)☒ A custom data source

Data source type:

Microsoft SQL Server

Connection string:

Data Source=[REDACTED] Initial
Catalog=AD_DW

Connect using:

☐ Credentials supplied by the user running the report

Display the following text to prompt user for a user name and password:

Type or enter a user name and password to access the data source

☐ Use as Windows credentials when connecting to the data source☐ Credentials stored securely in the report server

User name:

Password:

☐ Use as Windows credentials when connecting to the data source☐ Impersonate the authenticated user after a connection has been made☒ Windows integrated security☐ Credentials are not required[Test Connection](#)[Apply](#)