Setup ADchangeTracker instructions

Installation and configuration of ADchangeTracker overview

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

# Configure Event Logging in Active Directory

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

**You will need Domain Admin permissions to perform this task.**

*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](http://www.morgantechspace.com/2013/08/how-to-enable-active-directory-change.html)

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](http://www.morgantechspace.com/2013/08/active-directory-change-audit-events.html)

Here are a few other websites for reference:

[Who Moved the AD Cheese?](http://blogs.technet.com/b/askpfeplat/archive/2012/04/22/who-moved-the-ad-cheese.aspx)

[AD DS Auditing Step-by-Step Guide](https://technet.microsoft.com/en-us/library/cc731607(WS.10).aspx)

[Active Directory Services Audit - Document references](http://social.technet.microsoft.com/wiki/contents/articles/15232.active-directory-services-audit-document-references.aspx)

# Create service user in AD

**You will need Domain Admin permissions to perform this task.**

Create a user named “ad\_audit” in an OU where you normally keep service users.

# Grant service user permission to read Security Log on all DC‘s

**You will need Domain Admin permissions to perform this task.**

Click on “Builtin” OU in AD Users and Computers, double click “Event Log Readers” group. Add “ad\_audit” user to the group.

# Create security group for AD reports

**You will need Domain Admin permissions to perform this task.**

Create “SG-ADreports” security group in an OU where you normally keep such groups. Add all the users you want to have access to the AD reports.

# Create a database in SQL server

Bla

# Create logins and grant permissions in SQL server

Bla

# Install ADchangeTracker service on all writable DC‘s

**You will need Domain Admin permissions to perform this task.**

bla

# Configure service

bla

# Start service

bla

# Install and configure reports in SSRS































