NetWrix Active Directory Change Reporter

Quick Start Guide

Contents

Introduction

Active Directory change auditing is an important procedure for limiting unauthorized changes and errors to Active Directory configuration. One single change can put your organization at risk, introducing security breaches and compliance issues. Built-in Active Directory auditing lacks many important features (for example, it does not provide you the before and after values for changed properties) and does not have reporting capabilities. Careful analysis of multi-megabyte Security logs can take enormous resources and still never paint the whole picture.

NetWrix Active Directory Change Reporter is a tool that reports the changes made to Active Directory and delivers reports, containing summary and detailed information on a daily basis. These reports include the *4 W — Who, What, When,* and *Where* for all changes, plus *before* and *after* values for each of the settings, and also changes made to Active Directory configuration, schema, and other Active Directory objects.

You can use these reports to:

- Monitor day-to-day administrative activities.
- Prepare compliance reports for your SOX, GLBA and HIPAA auditors.

NetWrix Active Directory Change Reporter records all modifications, including both user and administrative activity, and e-mails daily reports to Active Directory administrators detailing every Active Directory change. Collected audit data is archived and can be stored for years, so you can build a summary of changes made to Active Directory during any period and drill down to detailed information as necessary. This archiving function allows organizations to analyze any policy violations, adhere to security best practices and maintain established internal policies.

Licensing

Active Directory Change Reporter comes in two versions: free and commercial. The table below outlines the differences between them.

Feature	Freeware Version	Commercial Version
Who and When fields for every change	No	Yes
Advanced reports based on SQL Reporting Services, with filtering, grouping and sorting	No	Yes. View report sample
Custom reports	No	Yes. Create manually or order from NetWrix
Enterprise-class scalability	Limited	Full
Long term archiving and reporting	Only for two days: today and yesterday	Any period of time
Technical support	Support forum	Phone, email
Licensing	Free of charge	Per enabled AD account or site license, please see our pricing information or request a quote

The free version can be used by businesses and individuals for an **unlimited** time, at no charge. The commercial version can be evaluated free of charge for **20** days.

Getting Started

Follow the instructions below to install and configure Active Directory Change Reporter.

System Requirements

The product can be installed on any computer running Windows XP SP2 or higher. The computer must belong to the managed domain.

Supported Active Directory environments:

- Windows 2000
- Windows Server 2003, any forest mode (mixed, native, 2K3)
- Windows Server 2008

Additional software:

- .Net Framework 2.0 or later
- Windows Installer 3.1 or later

Additional requirements:

- Disk space – enough for temporary data storage (the AD snapshots will be saved there). Required space depends on the number of users in your Active Directory and is calculated as follows:

  NumUsers*1 Kb

  For example, if you have 5000 users in your domain, you need at least 5MB of storage (daily collected data); to keep 1000 users data for 2 months, you need about 60MB of space (1K * 1000 * 60).

- The size of Security event logs on your domain controllers must be large enough to hold events for at least 36 hours. Otherwise, you may get incomplete information about who made some of the modifications. It is recommended to use Group Policy to adjust event logs sizes (for that, use **Administrative Tools | Domain Controller Security Policy**; configure log size in **Computer Configuration\Windows Settings\Security Settings\Event Log** node). The product reports conditions when one or more logs have been overwritten since the last collection (*).

- SQL Server 2005 or 2008 with Reporting Services (SSRS) are required for advanced reporting (*). SQL Server Express Edition with Advanced Services is supported; it can be installed and configured automatically. The following article explains how to configure SQL Server 2005 Express Edition to allow remote connections: http://support.microsoft.com/default.aspx?scid=kb;EN-US;914277

- SSRS Report Builder is required to create custom reports (*). To launch Report Builder, .NET Framework 2.0 must be installed on the client computer (used to connect to SSRS). Note that Report Builder is available in SQL Server Enterprise or Standard Edition; Express Edition does not provide this functionality.

(*) - feature is available in commercial version only.

Required rights and permissions

The account under which **NetWrix Active Directory Change Reporter** scheduled task will run requires the following:

1. Sufficient rights to query the entire Active Directory
2. **Content Manager** role for the **Home** folder on SSRS (*)
3. To collect and report on objects' security changes, this account must have **Manage auditing and security log** user right enabled (if the task is run under Domain Administrator account, this right will be enabled by default). Adjust Domain Controller Security Policy accordingly. (*)

The account you will use to view the reports in SSRS Report Manager should have the **Browser** role for the Home folder on SSRS. (*)

If you plan to collect data using agents (recommended; for details, see the product Help), consider that agent service will be run under Local System account. (*)

(*) - requirement applies to commercial version only.

Configuring AD Auditing (Required for Commercial Version Only)

Object-level AD auditing must be configured for ALL AD objects (not only domain controller objects or users making changes) to audit “Who/When” for all modifications (otherwise, Who/When information will not be reported). Open Active Directory Users and Computers snap-in and do the following:

1. From the main menu, select **View**, then select **Advanced Features** and make sure that the Active Directory Users and Computers Advanced mode is turned ON.
2. Right-click the root domain object, select **Security** tab, click **Advanced**, and select **Auditing** tab.
3. Click **Add** and type **Everyone**, then click **OK**.
4. Set the **Apply onto** setting as **This object and all child objects** (default).
5. Select all Successful Audit items except for the following: Full Control, List Contents, Read Permissions, Read All Properties
6. Click **OK**.

Auditing of the **Directory Service Access | Success** category must be turned ON for all domain controllers.

Important: DC policy (not a domain policy) must be used to enable this setting because domain controllers don't inherit domain policy settings by default.

To centrally enable this auditing setting:

1. Go to the Domain Controller Security Policy (available from the **Administrative Tools** menu on any DC), and navigate to **Computer Configuration | Windows Settings | Security Settings | Local Policies | Audit Policy** node
2. Make sure that **Audit directory service access** and **Audit account management** categories are set to **Success** (or **Success** and **Failure**).

If you want to monitor changes to domain Configuration and Schema containers, then you need to enable object-level auditing for these containers, using the following steps:

1. Run ADSI Edit utility (a part of the Windows Support Tools package)
2. Right-click the root node, select **Connect to**, and connect to the **Configuration** naming context of your domain.
3. Right-click the **Configuration** node for properties and go to the **Security** tab.
4. Click **Advanced** and select the **Auditing** tab.
5. Click **Add** and type *Everyone*, click **OK**.
6. In the **Apply onto** list, select **This object and all child objects**.
7. Select all **Successful Audit** items except for the following: **Full Control**, **List Contents**, **Read Permissions**, **Read All Properties**.

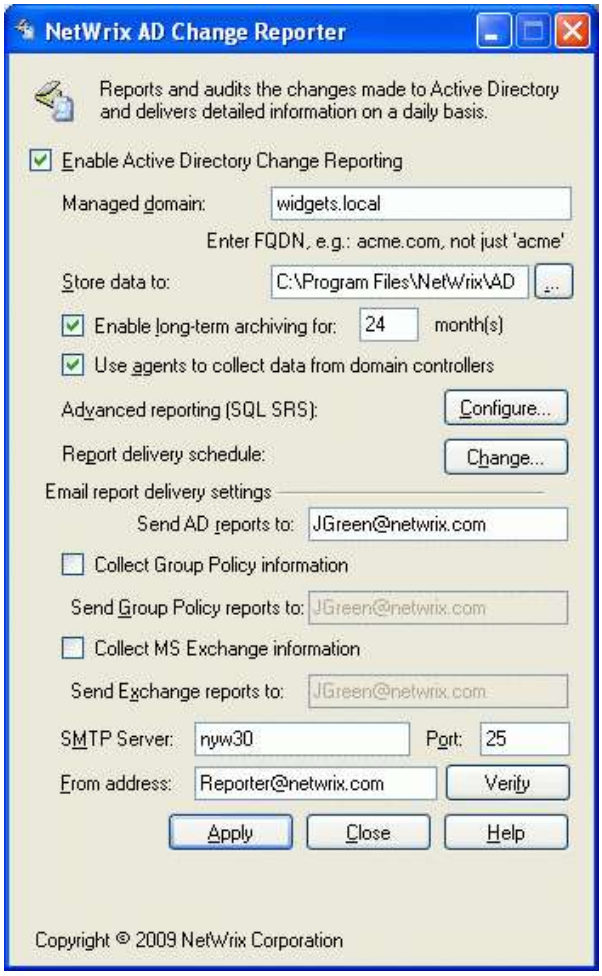
Important: Do NOT click the checkbox named **Apply these auditing to objects and/or containers within this container only**.

8. Click **OK**.
9. Repeat all steps above for the **Schema** container.

To report on password resets, auditing of the **Account Management | Success**category must be turned ON. Configuration instructions are the similar as those for Directory Service Access (see above).

Installation and Configuration

To install Active Directory Change Reporter, run the setup on the computer you have chosen. On the last step of the installation wizard, the configuration dialog box opens. Use it to specify configuration settings as follows:



- The **Enable Active Directory Change Reporting** check box is selected by default; when selected, the product generates the reports on AD changes and delivers them to the specified mailbox.
- Enter the Fully Qualified Name (FQDN) of the **Managed domain** which changes you want to track. For example, *mydepartment.myorganizaton.domain.com*, not just *mydepartment* or anything else.
- In **Store data to** field, enter the path for the folder where NetWrix Active Directory Change Reporter will store the Active Directory snapshots that contain domain data for tracking and analysis. Default setting (installation folder path) should be changed to the storage folder in your production environment; make sure the storage size meets the requirements stated above.

- To enable historical reporting, set the archiving depth; for that, select **Enable long-term archiving for** check box, and specify how long it should be saved for (months) (*).
- If required, select **Use agents to collect data from domain controllers** (*); this is a recommended option. For details on using agents, refer to product Help.
- To provide for advanced reporting (*) based on SQL Server Reporting Services (SSRS), click **Configure...**. For more details, see the product Help.
- Under **Email report delivery settings**, enter the e-mail addresses to send AD change reports to (multiple addresses should be separated by comma).
- You can modify schedule for the Windows task called **Netwrix Active Directory Change Reporter** that performs the collection of changes to AD, and e-mails the reports. By default, this task will be launched at 3 AM daily. To modify the schedule, click **Change...**.
- Supply SMTP server settings (name, port, and From address).

(*) - feature is available in commercial version only.

When you have finished with these settings, click **Apply**. You will be prompted for the credentials to run data collection and report generation. The account you specify will be used to run the **Netwrix Active Directory Change Reporter** scheduled task (it can also be launched manually, as described later in this document).

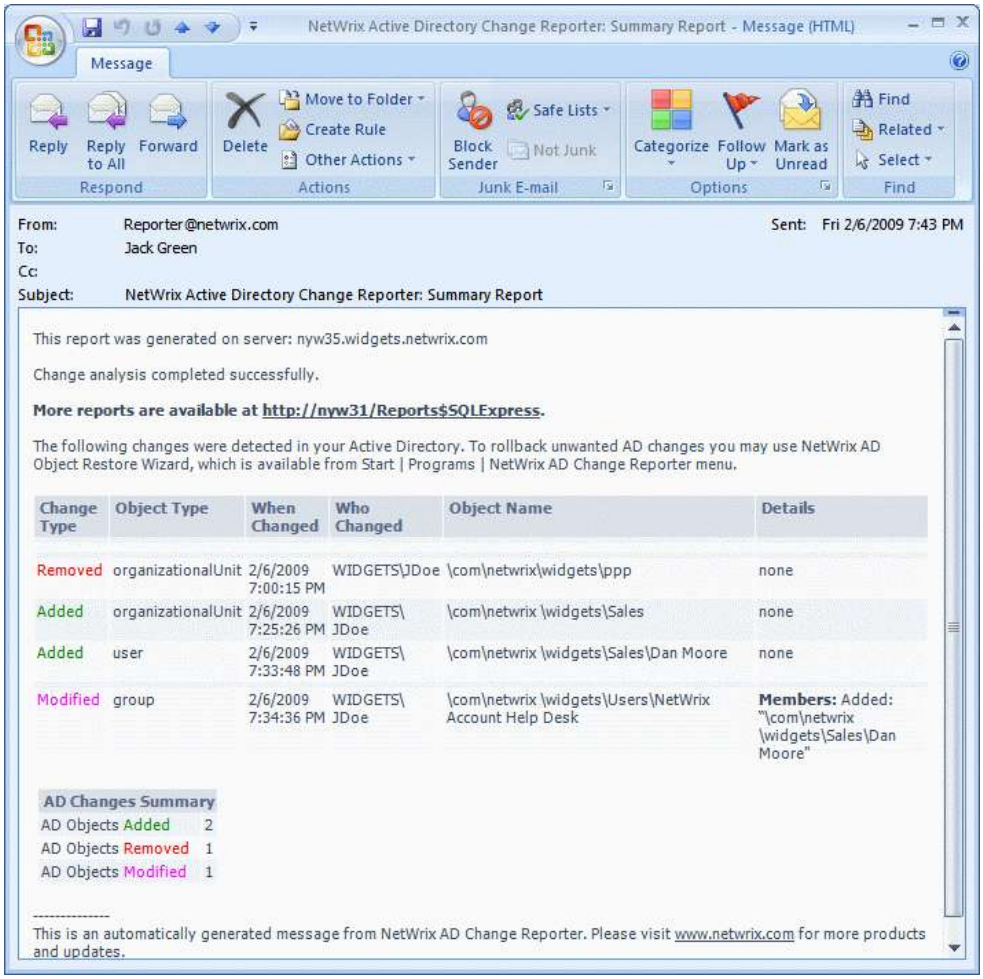
- The account must be powerful enough to query the entire Active Directory.
- To collect and report on object security changes, this account must have **Manage auditing and security log** user right enabled (if the task is run under Domain Administrator account, this right will be enabled by default). Adjust Domain Controller Security Policy accordingly.
- For advanced reporting to work properly, make sure that your user account and scheduled task account are assigned the Content Manager role for the SSRS Home folder.

Note: The last two requirements should be met if you are using the commercial version of the product.

The changes will take effect after you click **Apply** in the Configurator dialog. If necessary, you can later change configuration settings by invoking this dialog from the **Start** menu (select **NetWrix Active Directory Change Reporter** and then click **Configurator**).

Viewing the Reports

At the first run of the scheduled task, the message (e-mailed to the recipient specified during the configuration) notifies you of the initial analysis completed. Next, you can make some changes to your Active Directory to see how they will be reported. After that, you can launch the scheduled task again, and then check the mailbox for the new report. The changes should be reported like shown in the figure below; if so, consider the product installation and configuration completed.



If **Who changed** field reports *System* (instead of the change initiator's account), and you are running the commercial version of the product, then open the file attached to this e-mail and examine the auditing issues reported; to fix the issues, use the recommendations provided in the *Configuring AD Auditing* section of this guide.

Next Steps

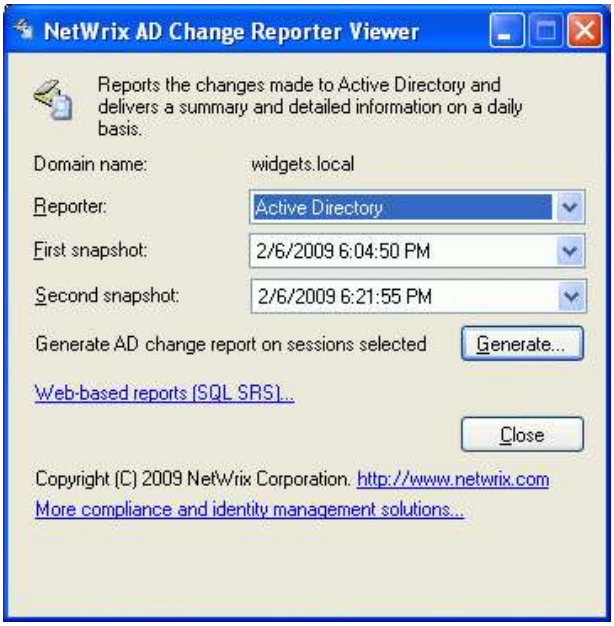
This section tells you how to manage Active Directory Change Reporter beyond the initial configuration. For more details, see the Active Directory Change Reporter help.

Running an On-Demand Report

To get a report on changes to Active Directory right away, you can select the **Netwrix Active Directory Change Reporter** in the list of the scheduled tasks, and select **Run** from its shortcut menu. The program will check for changes of Active Directory and automatically e-mail the report to the specified recipient(s).

Reporting on Changes That Occurred Between Two Snapshots

To view the changes that occurred between the particular snapshots, launch the **Report Viewer** from the Start menu.



Select the **Reporter** (i.e., the source that provides data for the report; for Active Directory Change Reporter this will be Active Directory). Then select the snapshots (by date) and click **Save** to generate and save a report on changes between them (in the HTM format). The report will be opened in the web browser to show you the changes that occurred between selected snapshots.

Note: Actually, this report will be identical to the report on changes you received by email at the time of the second snapshot generation.

Using SSRS-based Reporting (Commercial Version Only)

With SQL Server Reporting Services deployed, you can also configure advanced reporting (SSRS-based). In this case, you can use the advantages of SSRS-based reporting:

- Use the wide variety of reports to analyze the operation of your network environment; dozens of reports will help you to stay compliant with standards and regulations your organization is subject to (SOX, HIPAA, PCI, GLBA, SAS70, and others).
- Change the report filters to fine-tune the data view according to your needs.
- Use one of popular formats: PDF, XLS, etc. to save the report.
- Apply grouping and sorting to report data, and so on.

To use this type of reporting, you can either click **Configure** when supplying configuration settings during the setup, or invoke the Configurator later on. For details, see the product Help.

Additional Functionality

With **NetWrix Active Directory Change Reporter** deployed in your network environment, you can also generate the reports on changes to Group Policy and Exchange Server objects, as well as revert unwanted Active Directory changes. For details, refer to Group Policy Change Reporter Quick Start Guide, Exchange Server Change Reporter Quick Start Guide, and AD Object Restore Wizard Quick Start Guide.

How It Works

Typical **NetWrix Active Directory Change Reporter** data flow is described below.

1. AD infrastructure settings are periodically collected and stored to the specified storage as configuration snapshots. A report displaying changes to AD objects is sent to the specified e-mail recipient(s) and also can be viewed with SSRS Report Manager, as described in *Viewing Web-Based Reports* (*)

   (*) - Optionally, you can set up advanced reporting based on SQL Server Reporting Services as described in the product Help. Note that this functionality is available only in the commercial version of the product.

Note: If the database was not created during installation for this or that reason (for example, policy settings that require database admin privileges to create a database), run the **adcr_db.sql** script from installation folder using the account that has the required rights and privileges.

2. If SSRS-based reporting was configured for the product, then information about configuration changes is collected not only for a snapshot but is also automatically stored in the specified database and becomes available for report generation. You can view HTML reports in the SSRS Report Manager, or click the **More reports** link from the email report that you have received.

The **Netwrix Active Directory Change Reporter** collection and reporting workflow is usually as follows:

1. A user launches the Configurator and sets the parameters for automated data collection and reporting.

Note: Agents are recommended for data collection. Select the corresponding option in the Configurator to deploy the agents automatically (consider that agents usage is supported in commercial version only).

2. The Netwrix AD Change Reporter scheduled task is launched periodically (typically, every night, at 3 AM by default; it can also be launched manually when needed). This task collects configuration snapshots, and e-mails reports on changes and configuration to the specified recipients.
3. If SSRS-based reporting was configured, the task also stores information about configuration changes to the specified SQL server database (if automatic data import fails, you can use Database Importer to import data when necessary; see the product Help for details).
4. A user launches mail client to view the reports sent by e-mail; If SSRS-based reporting was configured, a user launches the web browser and views the reports in Report Manager.
5. To create custom reports, a user launches Report Builder and uses the existing model.