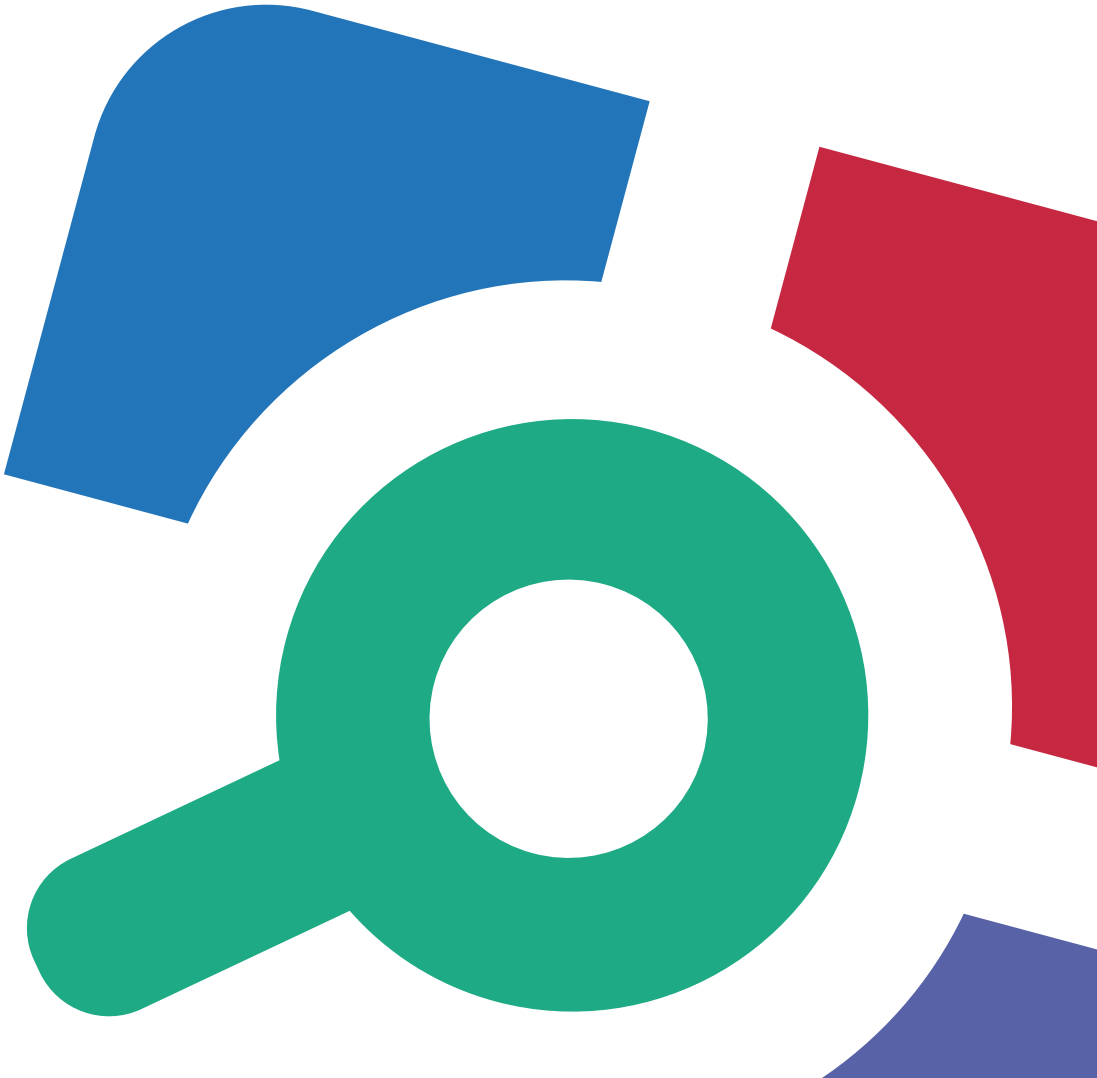
netwrix
#1 for change auditing

Netwrix Auditor for Active Directory

Quick-Start Guide

Product version: 6.0
5/8/2014



Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

Table of Contents

1. Introduction

This guide is intended for the first-time users of Netwrix Auditor for Active Directory. It can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided. After reading this guide you will be able to:

- Install and configure Netwrix Auditor
- Create a Managed Object for Active Directory Auditing
- Run data collection
- See how changes are reported

NOTE: This guide only covers basic configuration and usage options of the Active Directory Auditing feature. For advanced installation scenarios and configuration options, as well as for information on various reporting possibilities and other product features, refer to Netwrix Auditor Installation and Configuration Guide and Netwrix Auditor Administrator's Guide.

1.1. Netwrix Auditor Overview

Netwrix Auditor is a change and configuration auditing platform that streamlines compliance, strengthens security and simplifies root cause analysis across the entire IT infrastructure. It enables complete visibility by auditing changes made to security, systems and data.

Netwrix Auditor provides complete visibility into IT infrastructure changes with:

- Change auditing: determine *who* changed *what*, *when* and *where*.
- Configuration assessment: analyze current and past configurations with state-in-time reports.
- Predefined reports: pass audits with more than 200 out-of-the-box reports.

Netwrix Auditor employs AuditAssurance™, a patent-pending technology that does not have the disadvantages of native auditing or SIEM (Security Information and Event Management) solutions that rely on a single source of audit data. The Netwrix Auditor platform utilizes an efficient, enterprise-grade architecture that consolidates audit data from multiple independent sources with agentless or lightweight, non-intrusive agent-based modes of operation and scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years or more.

Powered by the Netwrix AuditAssurance™ technology, Netwrix Auditor makes the change auditing an easy and straightforward process, resulting in a complete and concise picture of all changes taking place in your monitored environment.

Netwrix Auditor for Active Directory includes the following features:

Netwrix Auditor Feature	Description
Active Directory Auditing	Netwrix Auditor allows tracking and reporting on all changes made to an AD domain, including the Domain, Configuration and Schema partitions. It also provides a built-in Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to the attribute level.
Event Log Management	Netwrix Auditor allows automatically consolidating, alerting and archiving even logs data. It collects Windows event logs and syslog events from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log data and rich reporting capabilities.
Group Policy Auditing	Netwrix Auditor allows tracking and reporting on all changes made to Group Policy configuration and Group Policy Objects.
Inactive User Tracking	Netwrix Auditor allows tracking inactive users and computer accounts. It performs the following tasks: • Checks domains or specific organizational units by inquiring all domain controllers, and notifies managers and administrators about accounts that have been inactive for a specified number of days. • Automatically deactivates inactive accounts by settings a random password, disabling, deleting or moving them to a specified organizational unit.
Password Expiration Alerting	Netwrix Auditor checks which domain accounts and/or passwords are to expire in a specified number of days and sends notifications to users via email or text messages (SMS). It also generates summary reports that can be delivered to system administrators and/or users managers. Netwrix Auditor also allows checking the effects of a password policy change before applying it to the managed domain.
User Activity Video Recording	Netwrix Auditor allows capturing a video of the users' activity on the monitored computers and writing a detailed activity log, which helps analyze how changes to your IT infrastructure are made. Netwrix Auditor allows searching inside video recordings and jumping to a specific timestamp to watch how certain actions were performed. It also provides detailed user activity reports; moreover, video records can be integrated into change reports of other Netwrix Auditor features.
Windows Server Auditing	Netwrix Auditor allows tracking and reporting on all changes made to

Netwrix Auditor Feature	Description
	your servers configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings and more.

1.2. Audited Systems

The table below lists all systems and applications that can be audited with the Netwrix Auditor for Active Directory solution that you are currently evaluating:

Netwrix Auditor Feature	Supported Versions
Active Directory Auditing	Domain Controller OS versions: • Windows Server 2003 (any forest mode: mixed/ native/ 2003) • Windows Server 2008 / 2008 R2 • Windows Server 2012
Event Log Management	Windows XP and above Syslog-based platforms: • Red Hat Enterprise Linux 5 • Ubuntu 11 • Ubuntu Server 11 • Any Linux system using Syslog (event collection rules must be created manually)
Group Policy Auditing	Domain Controller OS versions: • Windows Server 2003 (any forest mode: mixed/ native/ 2003) • Windows Server 2008 / 2008 R2 • Windows Server 2012
Inactive User Tracking	Domain Controller OS versions: • Windows Server 2003 (any forest mode: mixed/ native/ 2003) • Windows Server 2008 / 2008 R2 • Windows Server 2012
Password Expiration Alerting	Domain Controller OS versions:

Netwrix Auditor Feature	Supported Versions
	• Windows Server 2003 (any forest mode: mixed/ native/ 2003) • Windows Server 2008 / 2008 R2 • Windows Server 2012
User Activity Video Recording	Windows XP SP3 and above
Windows Server Auditing	Windows XP SP3 and above

2. Install Netwrix Auditor

2.1. System Requirements

2.1.1. Hardware Requirements

Before installing Netwrix Auditor, make sure that your hardware meets the following requirements:

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2GHz	Intel Core 2 Duo 2x 64 bit, 3GHz
Memory	2 GB RAM	8 GB RAM
Disk Space	500 MB physical disk space for the product installation. 1 GB for the Audit Archive. 500 MB for SQL Server databases to store the information on changes. **NOTE:** These are rough estimations, calculated for the Active Directory Auditing feature evaluation. Refer to Netwrix Auditor Installation and Configuration Guide for complete information on Netwrix Auditor disk space requirements.	
Screen resolution	1024 x 768	Screen resolution recommended by your screen manufacturer.

2.1.2. Software Requirements

The table below lists the minimum software requirements for the Netwrix Auditor installation:

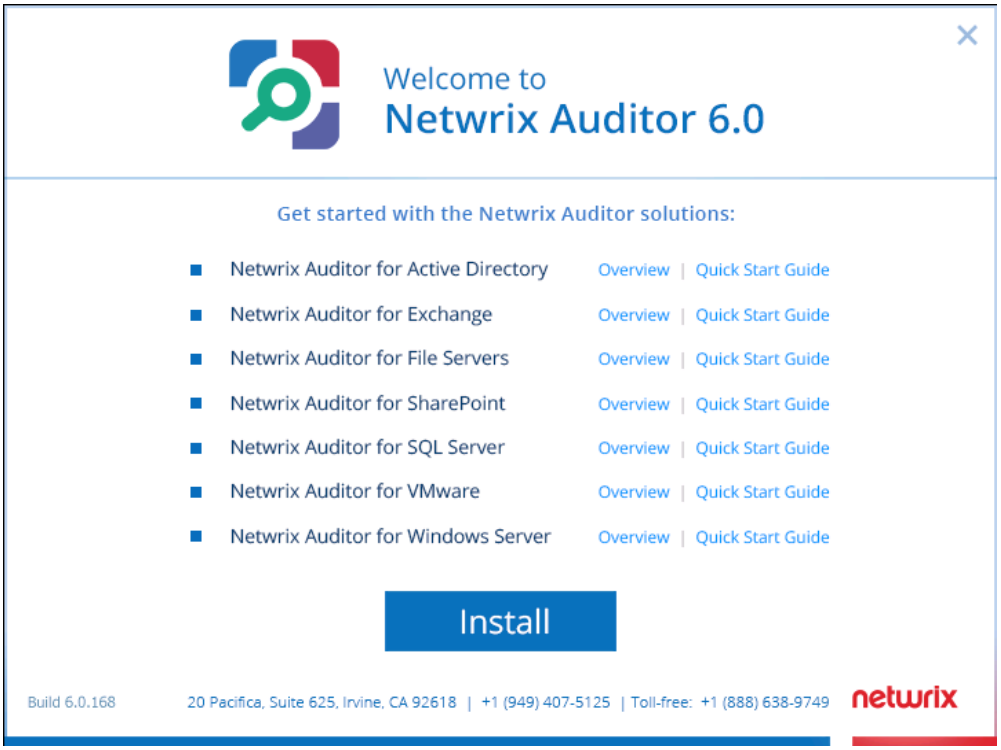
Component	Requirements
Operating system	• Windows 7 (32 and 64-bit) and above
.Net Framework	• .Net Framework 3.5 SP1
Additional Software	• Internet Explorer 7 and above • Windows Installer 3.1 and above

Component	Requirements
	• Windows Media Player (only required for the User Activity Video Recording feature) • Group Policy Management Console (only required for the Group Policy Auditing feature)

2.2. Install the Product

To install Netwrix Auditor

1. Download Netwrix Auditor 6.0.
2. Run the installation package. The following window will be displayed on successful operation completion:



3. Click **Install**. Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.

Netwrix Auditor shortcuts will be added to the **Start** menu and the Netwrix Auditor console will open.

3. Create Managed Object for Active Directory Auditing

To start auditing your IT Infrastructure with Netwrix Auditor you must create Managed Objects. The Managed Object is a container within the Netwrix Auditor console that stores information on your audited IT Infrastructure, the Data Processing Account used for data collection, auditing scope, reports delivery settings, etc.

1. Do one of the following:
   - In the Netwrix Auditor console main window select **Active Directory**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Domain** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Active Directory** as the audited system later in the wizard.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   Enter the default Data Processing Account (in the *domain_name\account_name* format) that will be used by Netwrix Auditor for data collection. This account must be granted at least the following rights and permissions:
   - Must be a member of the **local Administrators** group on the computer where Netwrix Auditor is installed.
   - If this account is going to be used to access the SQL database with audit data, it must also be granted **database owner (dbo_owner)** role.
   - Must have the **Log on as a batch job** policy defined. The **Log on as a batch job** policy will be automatically defined for the Data Processing Account as a local security policy.

     NOTE: If you have the **Deny log on as a batch job** policy defined locally or on the domain level, the local **Log on as a batch job** policy will not be applied. In this case, redefine the policy on the domain level through the **Group Policy Management** console.

   For a full list of rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summary delivery. Review the following for additional information:

Setting	Description
SMTP server	Enter your SMTP server name.

Setting	Description
Port	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the "From" field in Reports and Change Summaries. To check the email address, click **Verify**. The system will send a test message to the specified address and will inform you if any problems are detected.
SMTP Authentication	Select this check-box if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this check-box if your SMTP server requires SSL to be enabled.
Implicit SSL connection mode	Select this check-box if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

4. On the **Specify Domain Name** step, specify the target domain name in the FQDN format.
5. On the **Reports Settings** step, select **Enable Reports**.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2008 R2/ 2012 Express with Advanced Services. Refer to the following Netwrix Knowledge Base article: Which SQL Server versions can be installed automatically with Netwrix Auditor for detailed information on SQL Server versions that can be installed on your OS.
   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance.

Setting	Description
SQL Server instance	Specify the name of an existing SQL Server instance where a database for audit data will be created.
Windows Authentication	Select this option if you want to use the default Data Processing

Setting	Description
	Account to access the SQL database. This account must be granted **database owner (dbo_ owner)** role. Refer to Netwrix Auditor Installation and Configuration Guide for more information. If you want to use SQL Server Authentication, deselect this option.
User name	Specify the account to be used for SQL Server authentication. This account must be granted **database owner (dbo_owner)** role. Refer to Netwrix Auditor Installation and Configuration Guide for more information.
Password	Enter a password for the SQL Server authentication.
Report Server URL	Specify the Report Server URL. Click **Verify** to ensure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. Click **Verify** to ensure that the resource is reachable.

6. On the **State-in-Time Reports** step, you can enable or disable **State-in-Time Reports**. This feature allows generating reports on your system configuration state at a specific moment of time in addition to change reports. If enabled, the snapshots will be stored in the database. This option is unavailable if **Reports** were disabled.
7. On the **Select Data Collection Method** step, enable **Use Lightweight Agents**. If this feature is enabled, an agent will be installed automatically on target computers that will collect and pre-filter data and return it in a highly compressed format. This significantly improves data transfer and minimizes the impact on target computers performance.
8. On the **Configure Audit in Target Environment** step, select **Automatically for the selected audited systems**.
9. On the **Specify <your_audited_system> Change Summary Recipients** step, enter your email.

   NOTE: It is recommended to click **Verify**. The system will send a test message to the specified email address and inform you if any problems are detected.
10. On the **Configure Real-Time Alerts** step, leave the default settings.
11. On the last step, review your Managed Object settings and click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

4. Run Data Collection

When a new Managed Object is created, Netwrix Auditor starts collecting audit data from your environment. The first data collection creates an initial snapshot of the monitored system's current configuration state. Netwrix Auditor uses this information as a benchmark to collect data on changes to the audited environment. After the first data collection has finished, an email notification is sent to your email stating that the initial analysis has completed successfully. In order not to wait until a scheduled delivery, launch data collection manually.

To launch data collection manually

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** .
2. In the right pane, click **Run**.
3. Check your mailbox for email notification and make sure that data collection has completed successfully.

5. Make Test Changes

Now that the product has collected a snapshot of the audited system's current configuration state, you can make test changes to your environment to see how these changes will be reported.

For example, make the following test changes:

- Create a user using Active Directory Users and Computers
- Add this user to the **Domain Admins** group
- Disable any user account

NOTE: Before making any test changes to your environment, ensure that you have sufficient rights, and that the changes conform to your security policy.

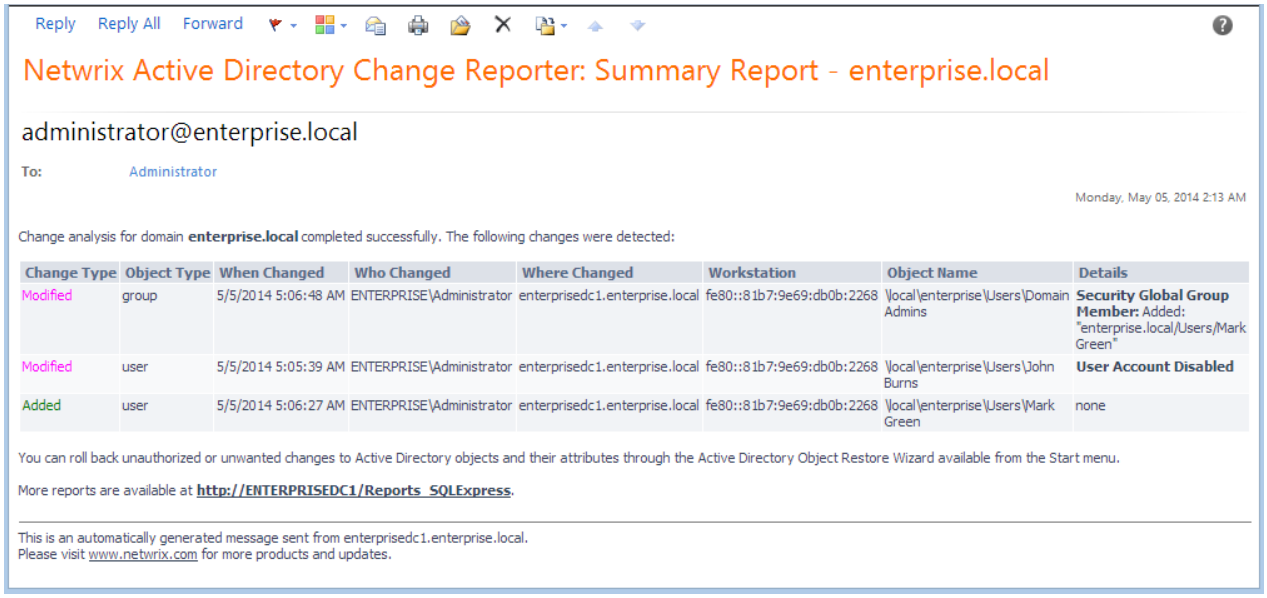
6. See How Changes Are Reported

6.1. Review Change Summary

After you have made test changes to your audited environment, you can see how these changes are reported. By default, a Change Summary is generated daily at 3:00 AM and delivered to the specified recipients. A Change Summary lists all changes / events / recorded user sessions that occurred since the last Change Summary delivery. In order not to wait until a scheduled delivery, launch data collection manually. See Run Data Collection for more information.

To review Change Summary

1. After the data collection has completed, locate the Change Summary email in your mailbox.
2. See how your changes are reported.



Reply Reply All Forward

Netwrix Active Directory Change Reporter: Summary Report - enterprise.local

administrator@enterprise.local

To: Administrator

Monday, May 05, 2014 2:13 AM

Change analysis for domain **enterprise.local** completed successfully. The following changes were detected:

Change Type	Object Type	When Changed	Who Changed	Where Changed	Workstation	Object Name	Details
Modified	group	5/5/2014 5:06:48 AM	ENTERPRISE\Administrator	enterprisedc1.enterprise.local	fe80::81b7:9e69:db0b:2268	\local\enterprise\Users\Domain Admins	**Security Global Group Member:** Added: "enterprise.local/Users/Mark Green"
Modified	user	5/5/2014 5:05:39 AM	ENTERPRISE\Administrator	enterprisedc1.enterprise.local	fe80::81b7:9e69:db0b:2268	\local\enterprise\Users\John Burns	**User Account Disabled**
Added	user	5/5/2014 5:06:27 AM	ENTERPRISE\Administrator	enterprisedc1.enterprise.local	fe80::81b7:9e69:db0b:2268	\local\enterprise\Users\Mark Green	none

You can roll back unauthorized or unwanted changes to Active Directory objects and their attributes through the Active Directory Object Restore Wizard available from the Start menu.

More reports are available at **http://ENTERPRISEDC1/Reports_SQLExpress**.

This is an automatically generated message sent from enterprisedc1.enterprise.local.
Please visit www.netwrix.com for more products and updates.

The example Change Summary provides the following information:

Parameter	Description
Change Type	Shows the type of action that was performed on the object.
Object Type	Shows the type of the object, for example, 'user'.
When Changed	Shows the exact time when the change occurred.
Who Changed	Shows the name of the account under which the change was made.
Where Changed	Shows the name of the domain controller where the change was made.

Parameter	Description
Workstation	Shows the name / IP address of the computer where the user was logged on when he made the change.
Object Name	Shows the path to the modified AD object.
Details	Shows the before and after values of the modified object, object attributes, etc.

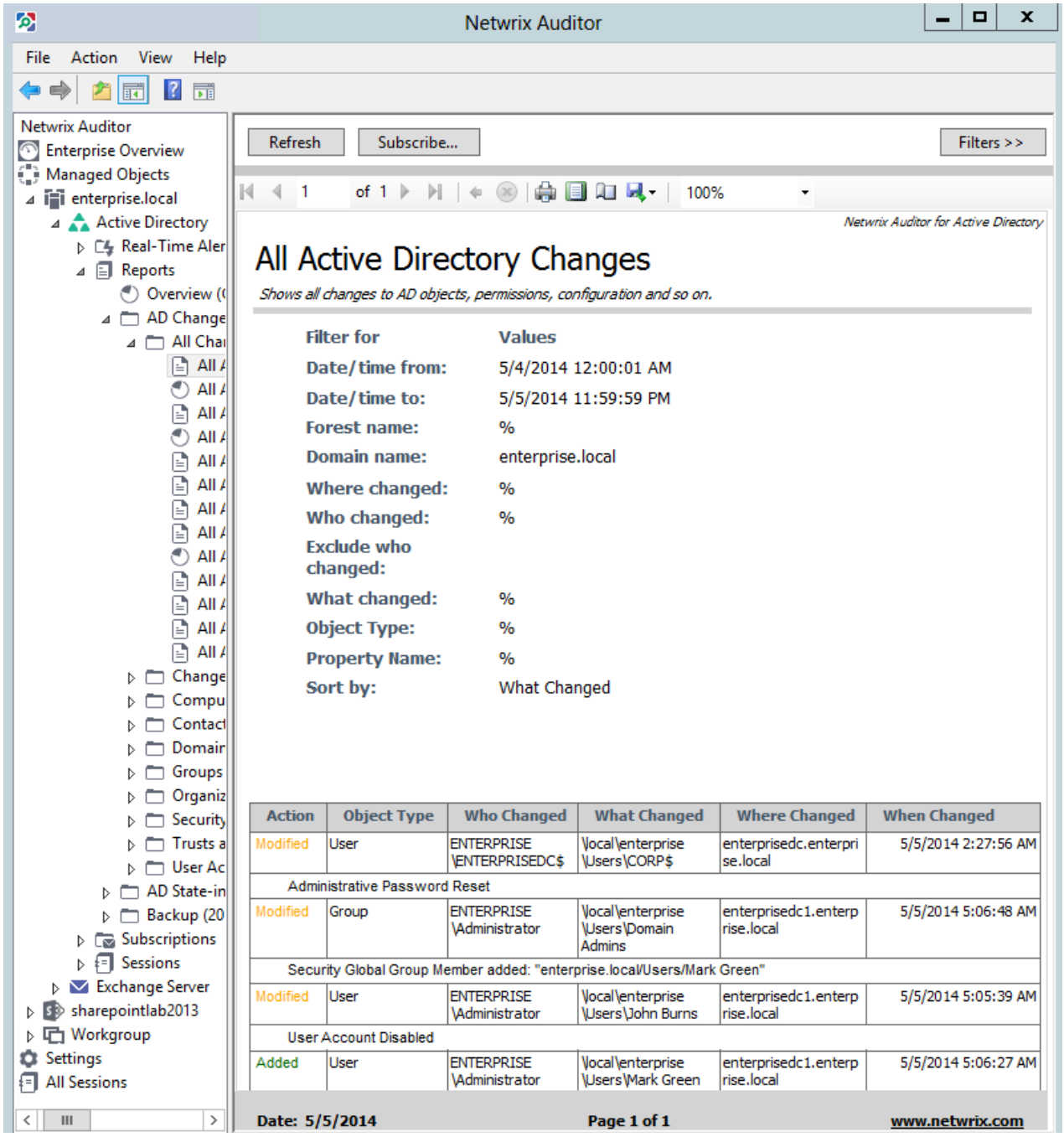
6.2. Review All Active Directory Changes Report

Netwrix Auditor allows generating audit reports based on Microsoft SQL Server Reporting Services (SSRS). The product provides a wide variety of predefined reports for each audited system that will help you keep track of all changes in your IT infrastructure and stay compliant with various standards and regulations (GLBA, HIPAA, PCI, SOX, etc.).

When you have launched initial data collection, made test changes to your environment and run data collection again you can take advantage of the Reports functionality.

To see how your changes are listed in the report

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Active Directory** → **Reports** → **AD Change Tracking** → **All Changes**.
2. Select the **All Active Directory Changes** report.
3. Click **View Report**. The report will be generated and displayed in the right pane.



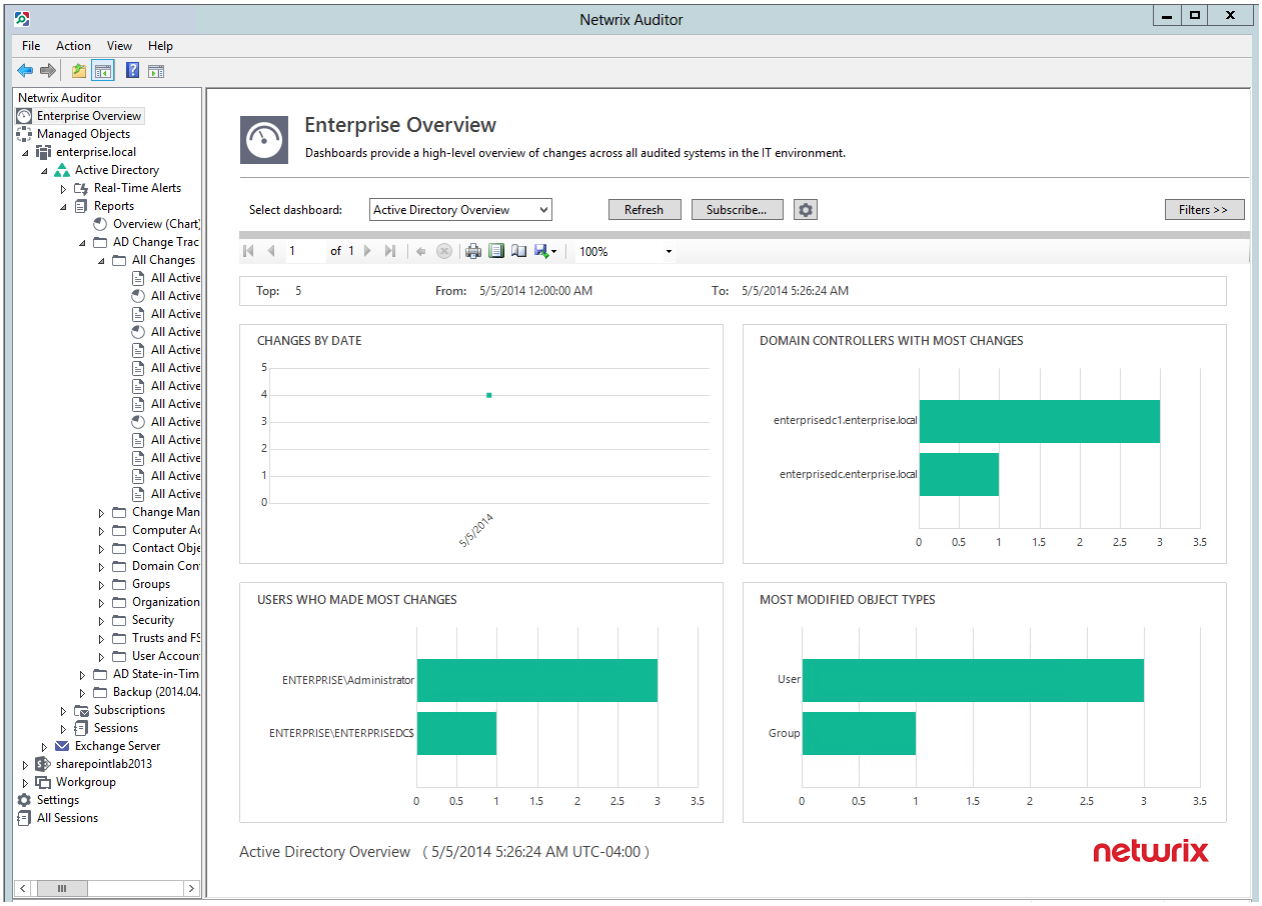
6.3. Review Changes With Active Directory Overview Dashboard

Dashboards provide a high-level overview of activity trends by date, user, server or audited system in your IT infrastructure. The Enterprise Overview dashboard aggregates data from all Managed Objects and all audited systems, while system-specific dashboards provide quick access to important statistics within one audited system.

When you have launched initial data collection, made test changes to your environment and run data collection again you can take advantage of **Active Directory Overview** dashboard.

To see how your changes are reported with Active Directory Overview dashboard

1. In the Netwrix Auditor console, navigate to **Enterprise Overview**.
2. In the right pane, select **Active Directory Overview** from the drop-down list next to **Select dashboard**.
3. Review your changes.
4. Click on any chart to proceed to the corresponding report.



7. Related Documentation

The table below lists all documents available to support Netwrix Auditor for Active Directory:

Document	Description
Netwrix Auditor Installation and Configuration Guide	Provides detailed instructions on how to install Netwrix Auditor, and explains how to configure your environment for auditing.
Netwrix Auditor Administrator's Guide	Provides a detailed explanation of the Netwrix Auditor features and step-by-step instructions on how to configure and use the product.
Netwrix Auditor Release Notes	Contains a list of the known issues that customers may experience with Netwrix Auditor 6.0, and suggests workarounds for these issues.

Index