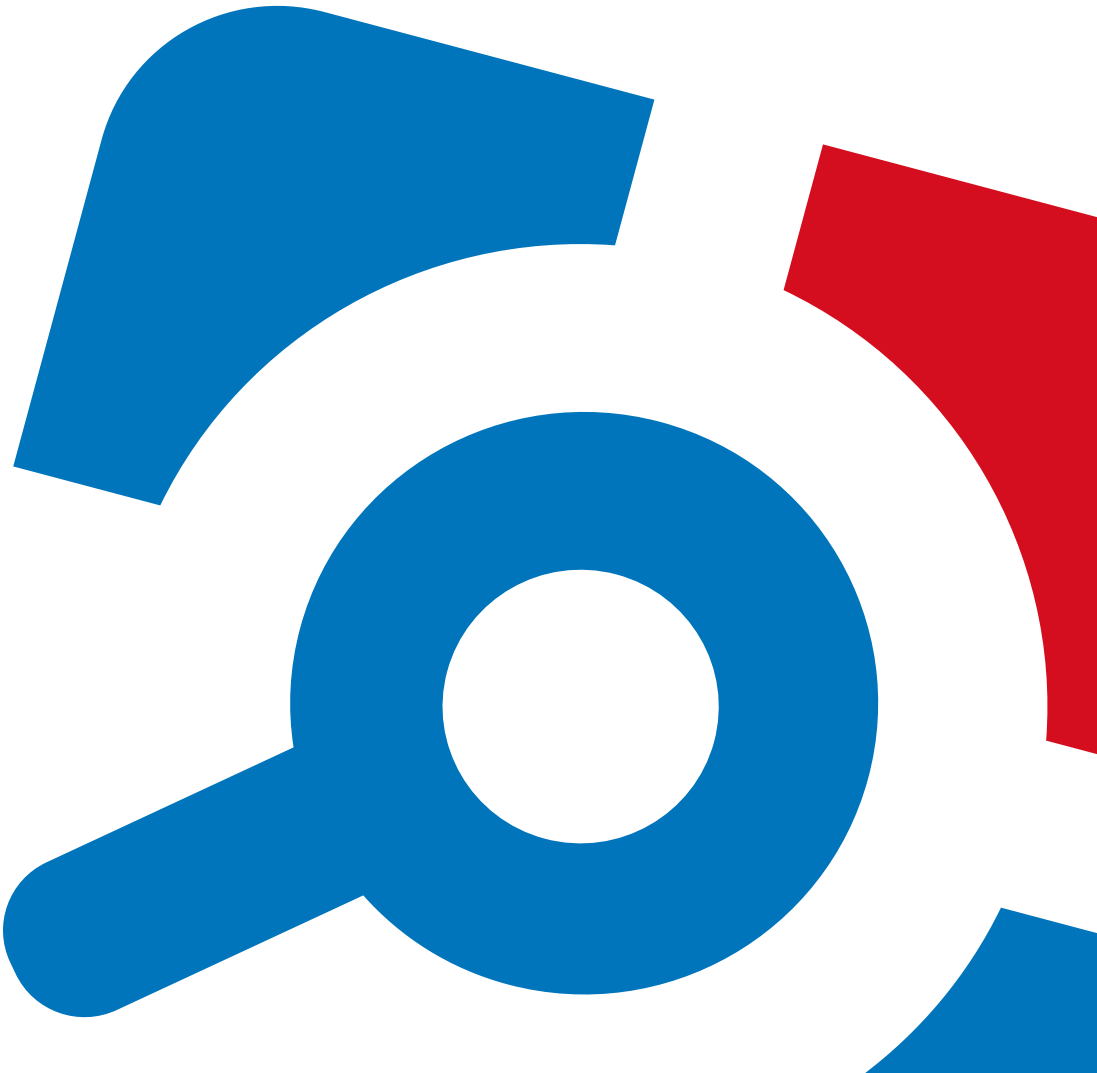
netwrix

Netwrix Auditor for Windows Server

Quick-Start Guide

Version: 8.0
4/22/2016



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.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

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 Windows Server. 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 to start auditing a Windows-based server
- Launch data collection
- See how Netwrix Auditor brings real AuditIntelligence into your IT infrastructure and enables its complete visibility

NOTE: This guide only covers the basic configuration and usage options for auditing Windows Server with Netwrix Auditor. 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
- Netwrix Auditor Administrator's Guide
- Netwrix Auditor User Guide

1.1. Netwrix Auditor Overview

Netwrix Auditor is an IT auditing platform that delivers complete visibility into changes and data access in hybrid cloud IT environments by providing actionable audit data about *who* changed *what*, *when* and *where* each change was made, and *who* has access to *what*. Netwrix Auditor helps organizations prevent security breaches caused by insider attacks, pass compliance audits with far less effort and expense, and keep tabs on what privileged users are doing in the environment.

Netwrix Auditor enables auditing of the broadest variety of IT systems, including Active Directory, Exchange, file servers, SharePoint, SQL Server, VMware and Windows Server. It also supports monitoring of privileged user activity in all other systems, even if they do not produce any logs, by enabling video recording of user screen activity and later search and replay. More than 160,000 IT departments worldwide rely on Netwrix Auditor to secure IT infrastructure, prove compliance and increase operational efficiency. The product has earned over 70 awards from leading industry publications, including SC Magazine, Windows IT Pro, Redmond Magazine and WindowSecurity.com.

Major benefits:

- **Change auditing and alerting:** Netwrix Auditor detects all configuration, content and security changes across your entire IT infrastructure. Reports and real-time alerts include the critical who, what, when and where details, including before and after values, enabling quick and effective

response.

- **AuditIntelligence interactive search:** Netwrix Auditor enables you to easily search through audit data and fine-tune sorting and filtering criteria so you can quickly hone in on exactly the information you need.
- **Configuration assessment:** State-in-time™ reports show configuration settings at any point in time, such as group membership or password policy settings as they were configured a year ago.
- **Access auditing:** Monitoring of and reporting on successful and failed access to systems and data helps keep sensitive data safe.
- **Predefined reports and diagrams:** Netwrix Auditor includes more than 150 predefined reports and diagrams. Reports can be exported to a range of formats, including PDF and XLS, and stakeholders can subscribe to reports to stay informed automatically by email.
- **AuditArchive™:** Netwrix Auditor's scalable two-tiered storage system (file-based + SQL database) holds consolidated audit data for more than 10 years.
- **Unified platform:** Many vendors require multiple standalone tools that are hard to integrate, but Netwrix Auditor is a unified platform that can audit the entire IT infrastructure.

Netwrix Auditor for Windows Server detects and reports on all changes made to Windows–based server configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings, DNS, and more. It also provides automatic consolidation and archiving of event logs data. Netwrix Auditor 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. In addition, Netwrix Auditor for Windows Server can be configured to capture a video of users' activity on the audited computers.

2. Netwrix Auditor System Requirements

This section lists the requirements for the systems that are going to be audited with Netwrix Auditor, and for the computer where the product is going to be installed.

2.1. Requirements for Audited System

The table below provides the requirements for the systems that can be audited with Netwrix Auditor for Windows Server:

Audited System	Supported Versions
Windows Server	• Windows Desktop OS (32 and 64-bit): Windows Vista SP2, Windows 7, Windows 8/ 8.1, and Windows 10 • Windows Server OS (32 and 64-bit): Windows Server 2008 SP2/2008 R2, Windows Server 2012/2012 R2

2.2. Requirements to Install Netwrix Auditor

This section provides the requirements for the computer where Netwrix Auditor is going to be installed. Refer to the following sections for detailed information:

- Hardware Requirements
- Software Requirements
- Deployment Options

2.2.1. 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, 2 GHz	Intel Core 2 Duo 2x 64 bit, 3 GHz Preferably a virtual machine

Hardware Component	Minimum	Recommended
RAM	2 GB	8 GB
Disk space	• 500 MB physical disk space for the product installation • 30 GB for the file-based Long-Term Archive • 500 MB for the SQL Server-based Audit Database where audit data is going to be stored **NOTE:** These are rough estimations, calculated for evaluation of Netwrix Auditor for Windows Server. Refer to Netwrix Auditor Installation and Configuration Guide for complete information on the Netwrix Auditor disk space requirements.	
Screen resolution	1280 x 1024	1920 x 1080 and higher

2.2.2. Software Requirements

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

Component	Requirements
Operating system	• Windows Desktop OS (64-bit): Windows 7 SP1, Windows 8/8.1 • Windows Server OS (64-bit): Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2
Framework	• .Net Framework 3.5 SP1

2.2.3. Deployment Options

Netwrix recommends to deploy Netwrix Auditor on any workstation in the domain where your audited system resides—installation on a domain controller is not recommended.

3. Review Components Checklist

To speed up the evaluation process, Netwrix recommends you to ensure that the following services and components are up and running prior to the Netwrix Auditor installation.

Service or component	Recommendations
Active Directory	Test Active Directory domain connectivity. Make sure your domain controllers are accessible from the computer where you intend to install Netwrix Auditor.
SQL Server 2014 with SSRS (optional step)	Although Netwrix Auditor provides a convenient interface for downloading SQL Server 2014 Express right from Netwrix Auditor Administrator Console, it is recommended to deploy SQL Server instance in advance. Test your SQL Server connectivity. **NOTE:** Netwrix Auditor provides an option to verify SSRS settings right in the Netwrix Auditor Administrator Console.

Test account	Netwrix recommends you to create a special account with extensive privileges. This account should have sufficient permissions to:
	• Collect audit data. See Configure Data Processing Account Rights and Permissions for more information.
	• Access data stored in the SQL Server instance:
	  • The account must be assigned the **Database owner (db_owner)** role and the **dbcreator** server role.
	  • The account must be assigned the **Content Manager** role on the SSRS Home folder.
	• Make test changes in your environment.

NOTE: There is no need to perform any additional configuration steps to prepare your IT infrastructure for auditing. Netwrix Auditor provides an option that automatically configures audit settings in the target environment. For a full list of settings required for Netwrix Auditor to collect comprehensive audit data and instructions on how to configure them manually, refer to Netwrix Auditor Installation and Configuration Guide.

3.1. Configure Data Processing Account Rights and Permissions

The Data Processing Account is used to collect audit data from the target systems.

In most cases, this account must be a member of the **Domain Admins** group, provided that the workstation with Netwrix Auditor installed and the audited system belong to the same domain.

If the computer where Netwrix Auditor is installed and the audited system belong to different workgroups or domains, the audited system must have accounts with the same name and password as the account under which Netwrix Auditor runs. All these accounts must belong to the **local Administrators** groups.

To ensure successful data collection the Data Processing Account must comply with the following requirements depending on the audited system.

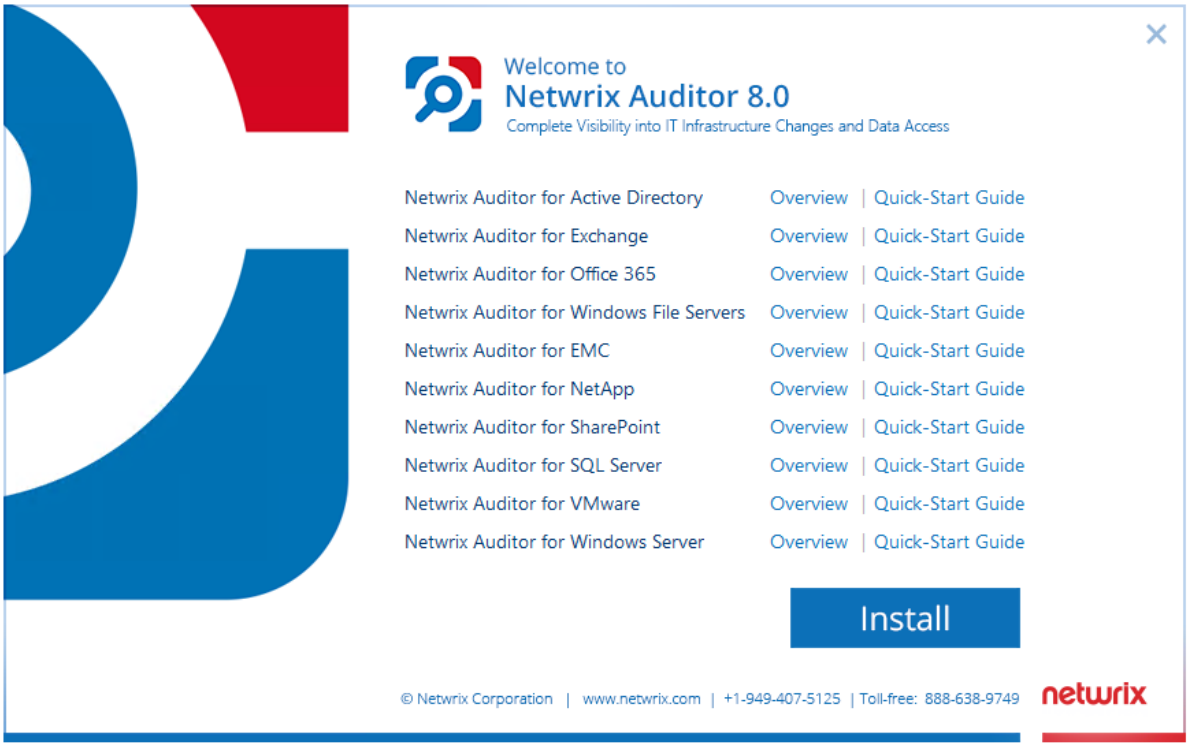
NOTE: The information in this section is outside the quick-start guide scope and is provided for reference only. See Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to configure your Data Processing Account.

Audited system	Rights and permissions
Windows Server (including DNS)	• A member of the **local Administrators** group If the computer where the product is installed and the audited servers belong to different domains, the target computers must have accounts with the same name and password as the Data Processing Account. All these accounts must be assigned the **local Administrators** permissions. • The **Log on as a batch job** policy defined for this account • The **Manage auditing and security log** policy must be defined for this account • The **Write** permission on the folder where the Long-Term Archive is going to be stored (by default *C:\ProgramData\Netwrix Auditor\Data*)

4. Install the Product

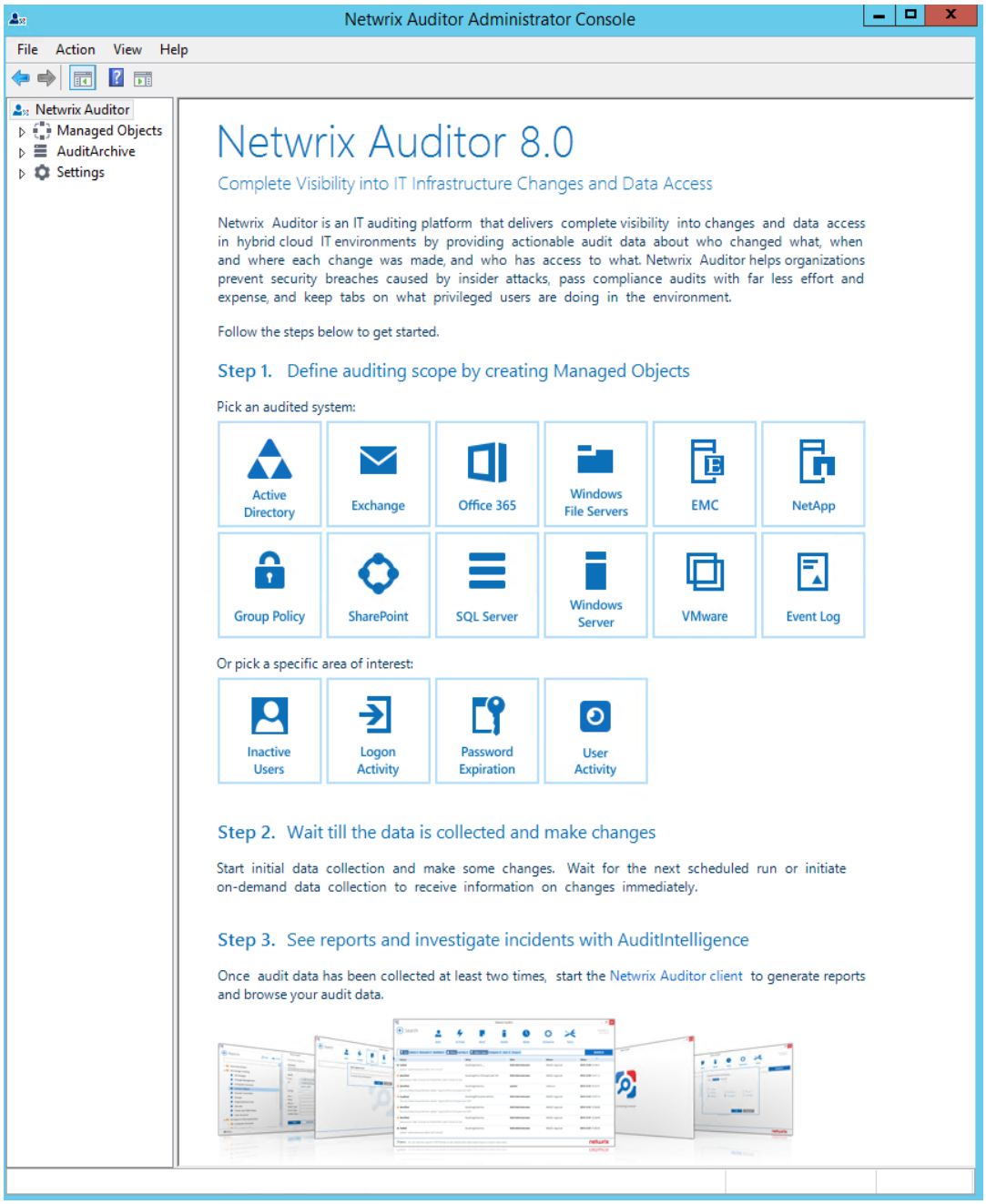
To install Netwrix Auditor

1. Download Netwrix Auditor 8.0.
2. Unpack the installation package. The following window will be displayed on successful operation completion:



3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, select **Full installation**.
5. On the **Destination Folder** step, specify the installation folder.
6. Click **Install**.

After a successful installation, Netwrix Auditor shortcuts will be added to the **Start** menu/screen and Netwrix Auditor Administrator Console will open.


Netwrix Auditor Administrator Console
File Action View Help
Netwrix Auditor
Managed Objects
AuditArchive
Settings
Netwrix Auditor 8.0
Complete Visibility into IT Infrastructure Changes and Data Access
Netwrix Auditor is an IT auditing platform that delivers complete visibility into changes and data access in hybrid cloud IT environments by providing actionable audit data about who changed what, when and where each change was made, and who has access to what. Netwrix Auditor helps organizations prevent security breaches caused by insider attacks, pass compliance audits with far less effort and expense, and keep tabs on what privileged users are doing in the environment.
Follow the steps below to get started.
Step 1. Define auditing scope by creating Managed Objects
Pick an audited system:
Active Directory
Exchange
Office 365
Windows File Servers
EMC
NetApp
Group Policy
SharePoint
SQL Server
Windows Server
VMware
Event Log
Or pick a specific area of interest:
Inactive Users
Logon Activity
Password Expiration
User Activity
Step 2. Wait till the data is collected and make changes
Start initial data collection and make some changes. Wait for the next scheduled run or initiate on-demand data collection to receive information on changes immediately.
Step 3. See reports and investigate incidents with AuditIntelligence
Once audit data has been collected at least two times, start the Netwrix Auditor client to generate reports and browse your audit data.

5. Create Managed Object to Audit Windows Server

To start auditing your IT Infrastructure with Netwrix Auditor, you must create a Managed Object. A Managed Object is a container within Netwrix Auditor that stores information on the auditing scope, the Data Processing Account used for data collection, Audit Database settings, etc.

1. On the main Netwrix Auditor Administrator Console page, click the **Windows Server** tile to launch the **New Managed Object** wizard.
2. On the **Select Managed Object Type** step, select **Computer Collection** as a Managed Object type.
3. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
4. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the **From** field. **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.
SMTP Authentication	Select this checkbox 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.

Setting	Description
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Implicit SSL connection mode	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

5. On the **Specify Computer Collection Name** step, enter the computer collection name.
6. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.
   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

   Complete the following fields:

Option	Description
	SQL Server Settings
SQL Server instance	Specify the name of the SQL Server instance to store audit data.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: • Windows authentication • SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance. **NOTE:** This account must be granted the **database owner (db_owner)** role and the **dbcreator** server role. See Netwrix Auditor Installation and Configuration Guide for more

Option	Description
	information.
Password	Enter a password.
SQL Server Reporting Services Settings	
Report Server URL	Specify the Report Server URL. Make sure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. Make sure that the resource is reachable.
User name	Specify the account to be used to connect to SSRS.
Password	Enter a password.

7. On the **Add Items to Computer Collection** step, select items that you want to audit. You can add several items to collection. Click **Add**, select an item type and add/browse for a computer name. Review the following for additional information:

Option	Description
Computer name	Allows specifying a single computer by entering its FQDN, NETBIOS or IP address. You can click **Browse** to select a computer from the list of computers in your network.
Active Directory container	Allows specifying a whole AD domain, OU or container. Click **Browse** to select from the list of containers in your network. You can also: • Select a particular computer type to be audited within the chosen AD container: **Domain controllers, Servers (excluding domain controllers)**, or **Workstations**. • Click **Exclude** to specify AD domains, OUs, and containers you do not want to audit. In the **Exclude Computers** dialog, click **Add** and specify an object. **NOTE:** The list of containers does not include child domains of trusted domains. Use other options (**Computer name, IP address range**, or **Import computer names from a file**) to specify the target computers.

Option	Description
IP address range	Allows specifying an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP range you want to exclude, and click **Add**.
Import computer names from a file	Allows specifying multiple computer names by importing a list from a .txt file (one computer name/IP address per line is accepted). You can choose whether to import the list once, or to update it automatically. If you select the **Import on every data collection** option, you can later modify the list of your audited computers by editing the .txt file. The audited computers list will be updated on the next data collection.

8. On the **Select Data Collection Method** step, enable **Network traffic compression**. If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.

   NOTE: If you disable the **Network traffic compression** option, you will not be able to configure audit automatically on the next step of the wizard.

9. On the **Configure Audit in Target Environment** step, select **Automatically for the selected audited systems**. Your current audit settings will be checked on each data collection and adjusted if necessary.

   NOTE: If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. For a full list of audit settings required for Netwrix Auditor to collect comprehensive audit data and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

10. On the **Select Monitored Systems Components** step, select the system components that you want to audit for changes.

11. On the **Configure Windows Server Change Summary Delivery Settings** step, specify the Change Summary recipients.

12. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

    When a new Managed Object is created, Netwrix Auditor starts collecting data from the audited IT infrastructure. The first data collection runs automatically and gathers information on the audited system's current configuration state. Netwrix Auditor uses this information as a benchmark to collect

data on changes. After the first data collection has finished, an email notification is sent to your email stating that the analysis has completed.

6. 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 see how they will be reported by Netwrix Auditor.

For example, make the following test changes:

- Modify a scheduled task
- Install a program

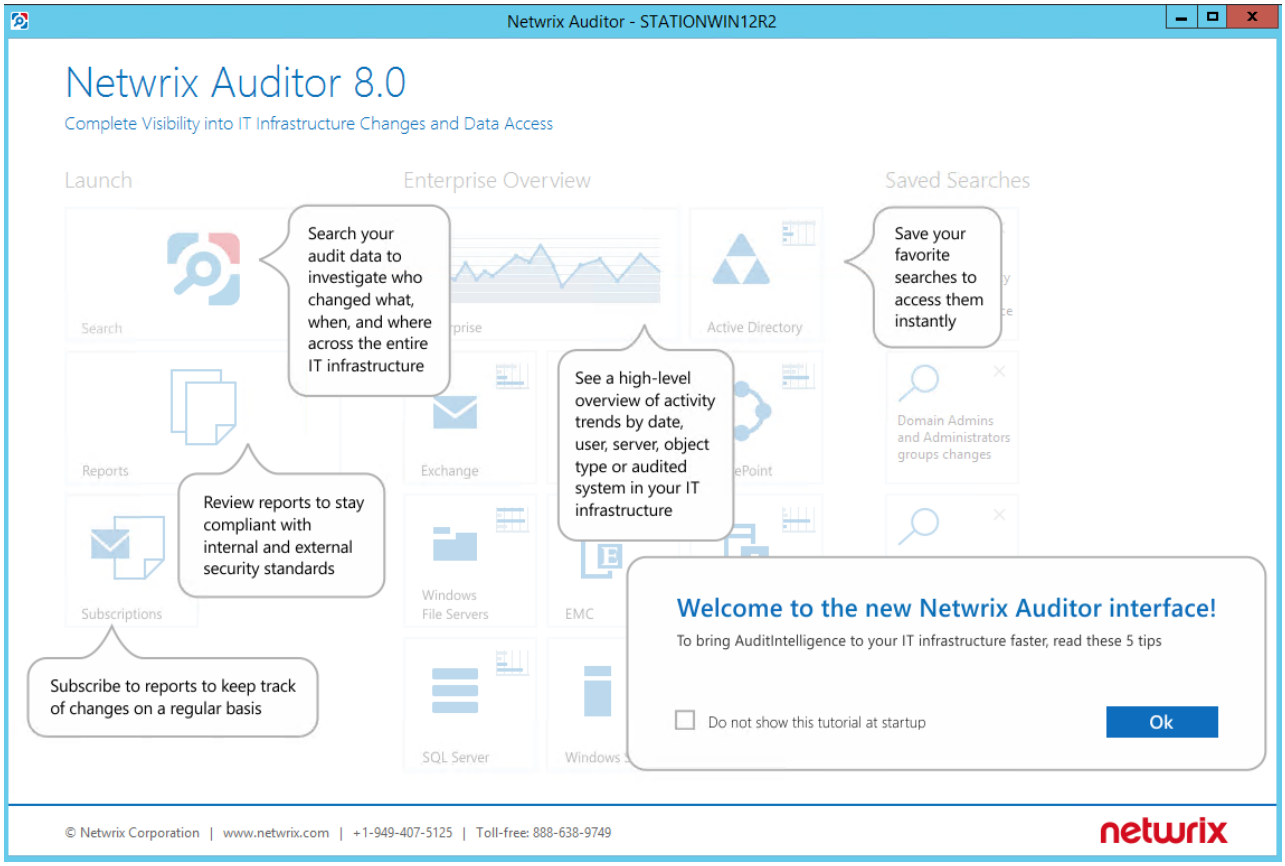
NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

7. See How Netwrix Auditor Enables Complete Visibility

After you have made test changes to the audited environment, you can see how Netwrix Auditor brings real AuditIntelligence into your IT infrastructure and enables its complete visibility. This section explains how to review your test changes in the Netwrix Auditor client and Change Summary.

To launch the Netwrix Auditor client

- Navigate to **Start** → **Netwrix Auditor**.



Review the following for additional information:

- Review a Change Summary
- Browse Data with AuditIntelligence Search
- Review Windows Server Overview
- Review the All Windows Server Changes Report

In order not to wait for a scheduled data collection and a Change Summary generation, launch data collection manually.

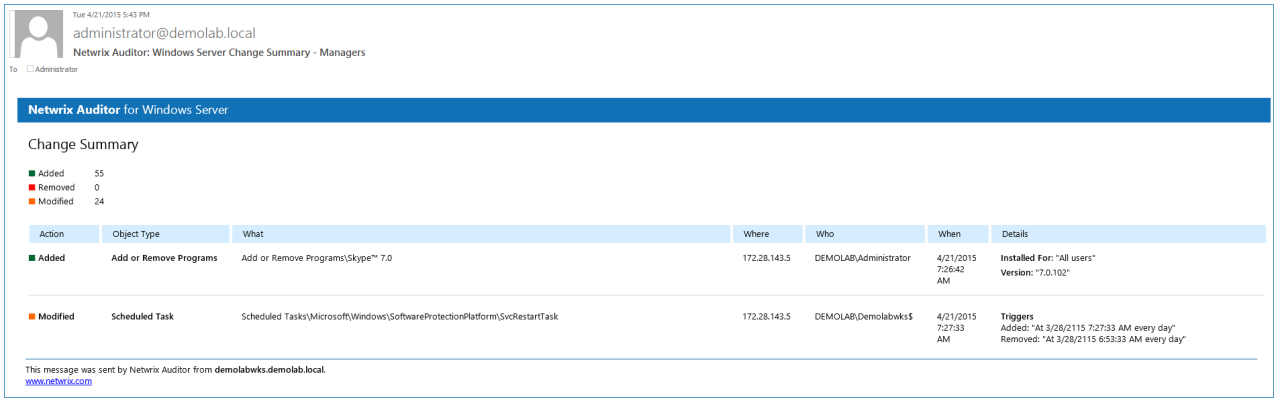
To launch data collection manually

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

7.1. Review a Change Summary

A Change Summary is email that lists all changes that occurred since the last Change Summary delivery. By default, a Change Summary is generated daily at 3:00 AM and delivered to the specified recipients. You can also launch data collection and a Change Summary generation manually.

After the data collection has completed, check your mailbox for a Change Summary and see how your test changes are reported:



The example Change Summary provides the following information:

Column	Description
Action	Shows the type of action that was performed on the object.
Object Type	Shows the type of the object.
What	Shows the name of the changed object or its path.
Where	Shows the name of the server where the change occurred.
Who	Shows the name of the account under which the change was made.

Column	Description
When	Shows the exact time when the change occurred.
Details	Shows the before and after values of the modified object, object attributes, etc.

7.2. Browse Data with AuditIntelligence Search

Netwrix Auditor delivers complete visibility into your IT infrastructure. Its convenient AuditIntelligence search interface enables you to investigate incidents and browse audit data collected across the entire IT infrastructure. When running a search in Netwrix Auditor, you are not limited to a certain audited system, change type, or object name. You can create flexible searches that provide you with precise results on *who* changed *what*, *when* and *where*.

After collecting initial data, making test changes to your environment and running data collection again, you can take advantage of AuditIntelligence search.

To browse your audit data and see you test changes

1. On the main Netwrix Auditor page, navigate to **Search**.
2. Add search filters to your search by clicking on a corresponding icon and providing a value. By default, all entries that contain this filter value are shown. For an exact match, use quotation marks.

   Filters are used to narrow your search results. To create a unique set of filters, you can:

   - Add different filters to your search. Search results will be sorted by all selected filters since they work as a logical conjunction (e.g., **Who***: Administrator* AND **Action***: Added*).
   - Specify several values in the same filter to search for any of them (e.g., **Action***: Modified* OR **Action***: Removed*). To do this, select a filter again and specify a new value.

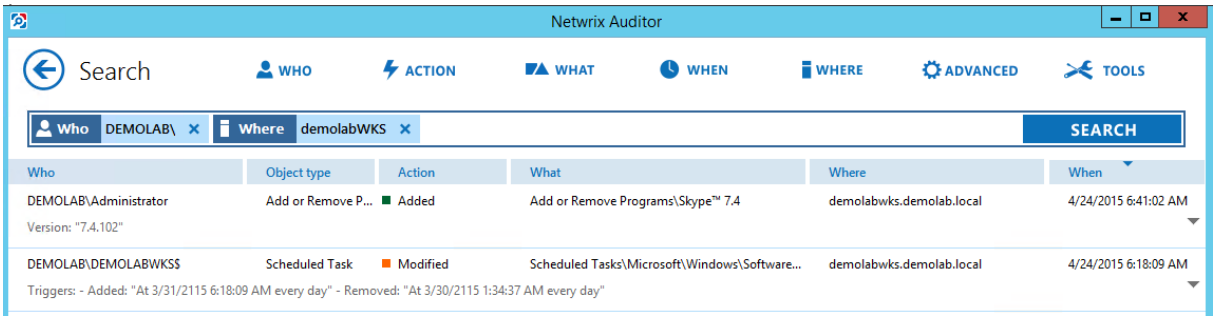
   For example, consider adding these filters:

Filter	Value
 WHO	Specify your account name, as you performed test changes. As some scheduled tasks are managed under system account, you can provide just a domain name, Netwrix Auditor will search across all accounts that contain it.
 WHERE	Specify your server name.

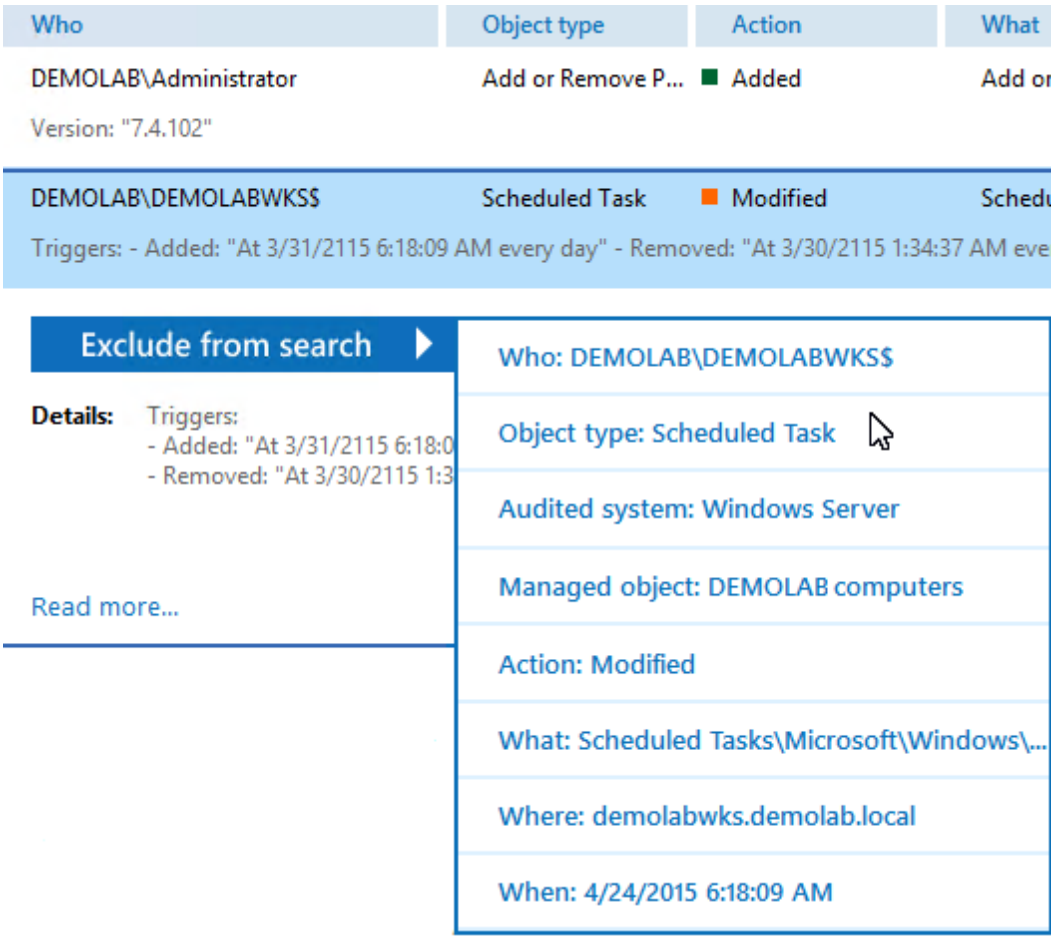
NOTE: Refer to Netwrix Auditor User Guide for detailed instructions on how to apply filters and change match types.

As a result, you will see the following filters in the **Search** field:

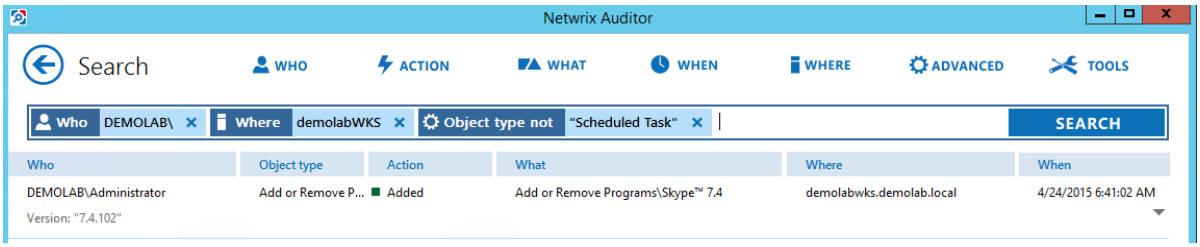
3. Click **Search**.



4. Now, you can narrow your search and modify it right from the search results pane. Double-click any entry that contains excess data, select **Exclude from search** and specify a filter, e.g., **Object type**: *Scheduled Task* to leave information on program installations and uninstallations only.



Your **Search** field will be updated, the **Object type not** filter will be added. Make sure to click **Search** again to update your search results.



5. Having reviewed your search results, navigate to **Tools**.
   - Click **Export data** to save your search results as a *.pdf or *.csv file.
   - Click **Save search** to save the selected set of filters. This search will be added to the **Saved Searches** section on the main Netwrix Auditor page, so that you will be able to access it instantly. Refer to Netwrix Auditor User Guide for detailed instructions on how to create saved searches.

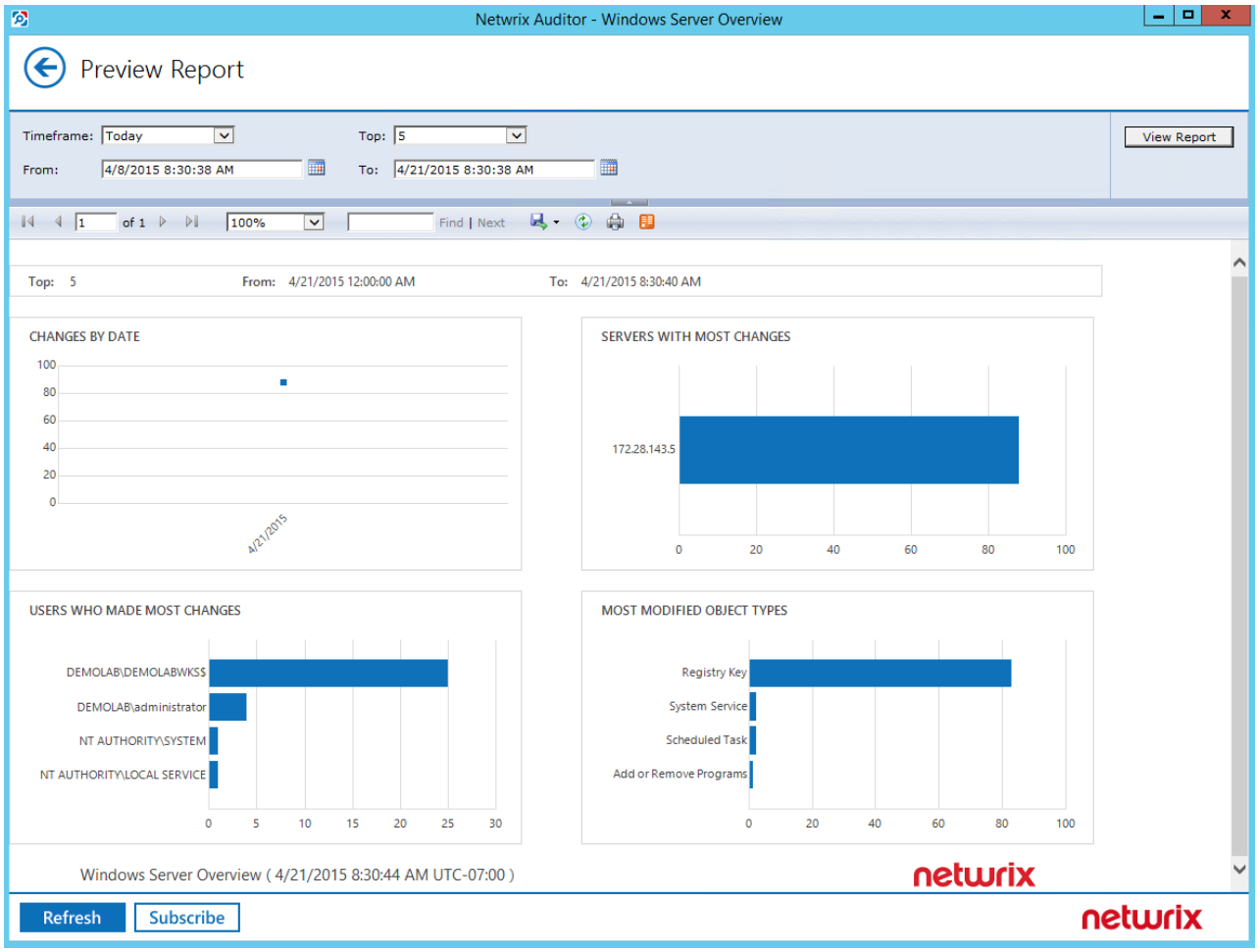
7.3. Review Windows Server Overview

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

After collecting initial data, making test changes to your environment and running data collection again, you can take advantage of the **Windows Server Overview**.

To see how your changes are reported with Windows Server Overview

1. On the main Netwrix Auditor page, navigate to the **Enterprise Overview** section.
2. Click the **Windows Server** tile to open it.
3. Review your changes.
4. Click on any chart to jump to a table report with the corresponding grouping and filtering of data.



7.4. Review the All Windows Server Changes Report

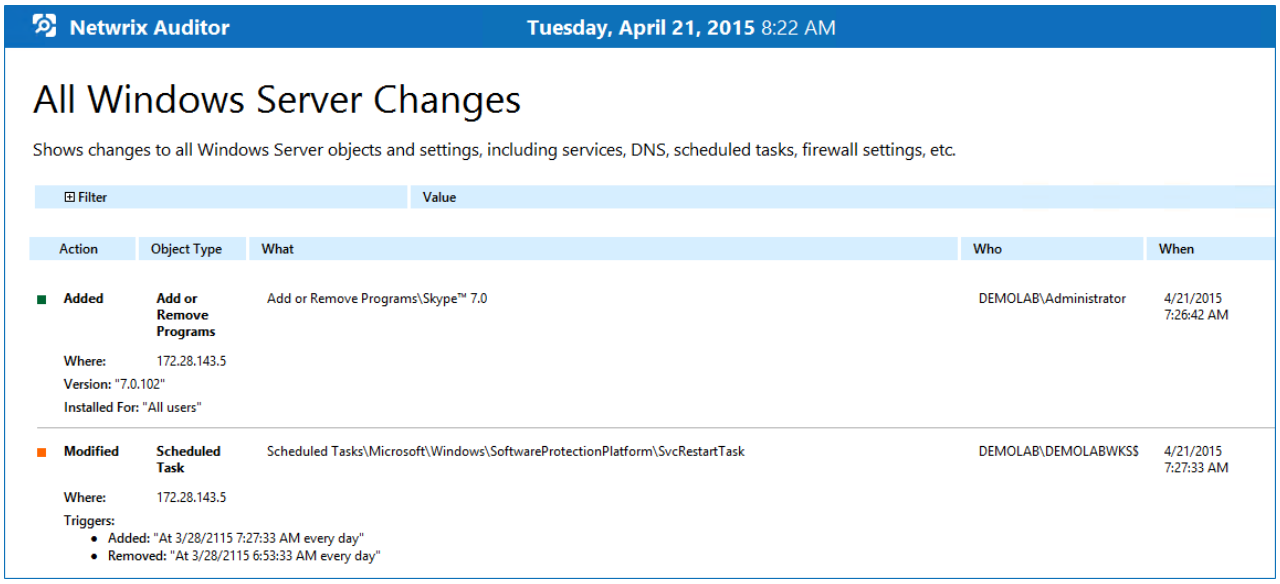
Netwrix Auditor allows generating audit reports based on Microsoft SQL Server Reporting Services (SSRS). The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure, an individual system, or a Managed Object.

Change reports can be found under the **Reports** → **Windows Server** and provide a narrower insight into what is going on in the audited infrastructure and help you stay compliant with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.).

After collecting initial data, making test changes to your environment and running 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 client, navigate to **Reports** → **Windows Server** → **Windows Server Changes**.
2. Select the **All Windows Server Changes** report.
3. Click **View** to open the report.



Netwrix Auditor Tuesday, April 21, 2015 8:22 AM

All Windows Server Changes

Shows changes to all Windows Server objects and settings, including services, DNS, scheduled tasks, firewall settings, etc.

Filter | Value

Action	Object Type	What	Who	When
Added	**Add or Remove Programs**	Add or Remove Programs\Skype™ 7.0	DEMOLAB\Administrator	4/21/2015 7:26:42 AM
Where: 172.28.143.5 Version: "7.0.102" Installed For: "All users"				
Modified	**Scheduled Task**	Scheduled Tasks\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask	DEMOLAB\DEMOLABWKS$	4/21/2015 7:27:33 AM
Where: 172.28.143.5 Triggers: • Added: "At 3/28/2115 7:27:33 AM every day" • Removed: "At 3/28/2115 6:53:33 AM every day"				

8. Related Documentation

The table below lists all documents available to support Netwrix Auditor for Windows Server:

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 step-by-step instructions on how to configure and use the product.
Netwrix Auditor User Guide	Provides detailed instructions on how to enable complete visibility with AuditIntelligence.
Netwrix Auditor Integration API Guide	Provides step-by-step instructions on how to leverage Netwrix Auditor audit data with on-premises and cloud auditing solutions using RESTful API.
Netwrix Auditor Release Notes	Lists the known issues that customers may experience with Netwrix Auditor 8.0, and suggests workarounds for these issues.