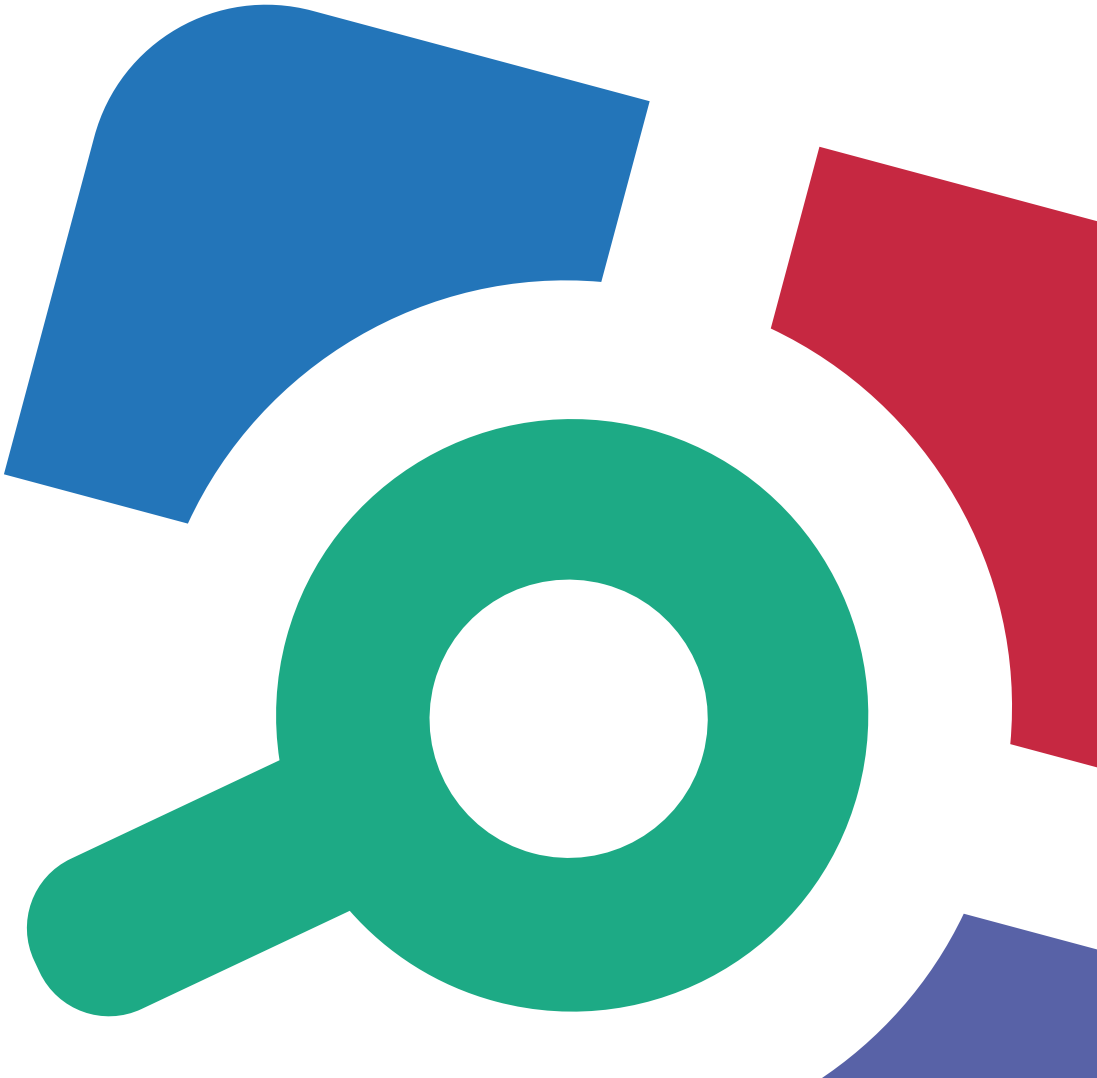
netwrix
#1 for change auditing

Netwrix Auditor

Administrator's 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.

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. Active Directory is a trademark of Microsoft Corporation. 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. Netwrix Auditor Overview

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 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.
EMC Storage Auditing	Netwrix Auditor allows tracking and reporting on all changes made to EMC VNX/VNXe/Celerra storage appliances, including files, folders and permissions, as well as failed and successful access attempts.
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

Netwrix Auditor Feature	Description
	event log data and rich reporting capabilities.
Exchange Server Auditing	Netwrix Auditor allows tracking and reporting on all changes made to Microsoft Exchange Server configuration and permissions.
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.
NetApp Filer Auditing	Netwrix Auditor allows tracking and reporting on all changes made to NetApp Filer CIFS shares, permissions, as well as failed and successful access attempts.
Mailbox Access Auditing	Netwrix Auditor allows tracking all non-owner mailbox access events in an Exchange organization, and immediately notifying users whose mailboxes have been accessed by non-owners.
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.
SharePoint Auditing	Netwrix Auditor allows tracking and reporting on all changes made to SharePoint farms, servers and sites, as well as their settings and permissions.
SQL Server Auditing	Netwrix Auditor allows tracking and reporting on all changes made to your SQL Servers configuration and database content.
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

Netwrix Auditor Feature	Description
	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.
VMware Auditing	Netwrix Auditor allows tracking and reporting on all changes made to your ESX servers, folders, clusters, resource pools, virtual machines and their hardware.
Windows File Server Auditing	Netwrix Auditor allows tracking and reporting on all changes made to Windows file servers, including files, folders, shares and permissions, as well as failed and successful access attempts.
Windows Server Auditing	Netwrix Auditor allows tracking and reporting on all changes made to 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:

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
EMC Storage Auditing	EMC VNX/VNXe/Celerra families (CIFS configuration only)
Event Log Management	Windows XP and above Syslog-based platforms: • Red Hat Enterprise Linux 5 • Ubuntu 11 • Ubuntu Server 11

Netwrix Auditor Feature	Supported Versions
	• Any Linux system using Syslog (event collection rules must be created manually)
Exchange Server Auditing	Exchange Server 2003 Exchange Server 2007 Exchange Server 2010 Exchange Server 2013
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
NetApp Filer Auditing	NetApp Filer (CIFS configuration only)
Mailbox Access Auditing	Exchange Server 2003 Exchange Server 2007 Exchange Server 2010
Password Expiration Alerting	Domain Controller OS versions: • Windows Server 2003 (any forest mode: mixed/ native/ 2003) • Windows Server 2008 / 2008 R2 • Windows Server 2012
SharePoint Auditing	SharePoint Foundation 2010 and SharePoint Server 2010 SharePoint Foundation 2013 and SharePoint Server 2013
SQL Server Auditing	SQL Server 2000 SQL Server 2005 SQL Server 2008

Netwrix Auditor Feature	Supported Versions
	SQL Server 2008 R2 SQL Server 2012
User Activity Video Recording	Windows XP SP3 and above
VMware Auditing	VMware ESXi 4.x and above vSphere vCenter 4.x and above
Windows File Server Auditing	Windows XP SP3 and above
Windows Server Auditing	Windows XP SP3 and above

1.3. Product Editions

The table below outlines the features that are included in the Netwrix Auditor solutions:

Solution	Feature
Netwrix Auditor for Active Directory	Active Directory Auditing Group Policy Auditing Event Log Management Inactive User Tracking Password Expiration Alerting User Activity Video Recording Windows Server Auditing
Netwrix Auditor for Exchange	Event Log Management Exchange Server Auditing Mailbox Access Auditing User Activity Video Recording Windows Server Auditing
Netwrix Auditor for File Servers	EMC Storage Auditing Event Log Management NetApp Filer Auditing

Solution	Feature
	User Activity Video Recording
	Windows File Server Auditing
	Windows Server Auditing
Netwrix Auditor for SharePoint	Event Log Management
	SharePoint Auditing
	User Activity Video Recording
	Windows Server Auditing
Netwrix Auditor for SQL Server	Event Log Management
	SQL Server Auditing
	User Activity Video Recording
	Windows Server Auditing
Netwrix Auditor for VMware	Event Log Management
	User Activity Video Recording
	VMware Auditing
	Windows Server Auditing
Netwrix Auditor for Windows Server	Event Log Management
	User Activity Video Recording
	Windows Server Auditing

1.4. How It Works

Depending on monitored system a typical Netwrix Auditor data collection and reporting workflow may include the following steps:

1. An administrator configures Managed Objects and sets the parameters for automated data collection and reporting.
2. Netwrix Auditor monitors the target system and collects audit data on changes and point-in-time configuration snapshots. Audit data is written to a local file-based storage, referred to as the Audit Archive.
3. If an event is detected that triggers an alert, an email notification is sent immediately to the specified recipients.

4. If the Reports functionality is enabled and configured, data is imported from the Audit Archive to a dedicated SQL database. Reports based on audit data can be viewed via the Netwrix Auditor console, or in a web browser, or delivered automatically on a specified scheduled if a subscription is configured.
5. The product emails Change Summaries that list all changes occurred in the last 24-hours to the specified recipients daily at 3:00 AM by default.

2. Start Auditing Your IT Infrastructure With Managed Objects

2.1. Managed Objects Overview

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.

Depending on the system you want to audit, Netwrix Auditor allows creating the following Managed Object types:

Managed Object	Feature
Domain	Active Directory Auditing
	Group Policy Auditing
	Exchange Server Auditing
	Inactive User Tracking
	Password Expiration Alerting
Computer Collection	Event Log Management
	User Activity Video Recording
	Windows File Server Auditing
	Windows Server Auditing
	SQL Server Auditing
Organizational Unit	Inactive User Tracking
	Password Expiration Alerting
VMware Virtual Center	VMware Auditing
SharePoint Farm	SharePoint Auditing

The following features do not require a Managed Object to audit your IT Infrastructure:

- Mailbox Access Auditing
- EMC Storage Auditing
- NetApp Filer Auditing

2.1.1. Group Managed Objects

For your convenience, you can group Managed Objects into folders. To create a folder, navigate to the **Managed Objects** node, right-click it, select **Create New Folder**, and specify the folder name.

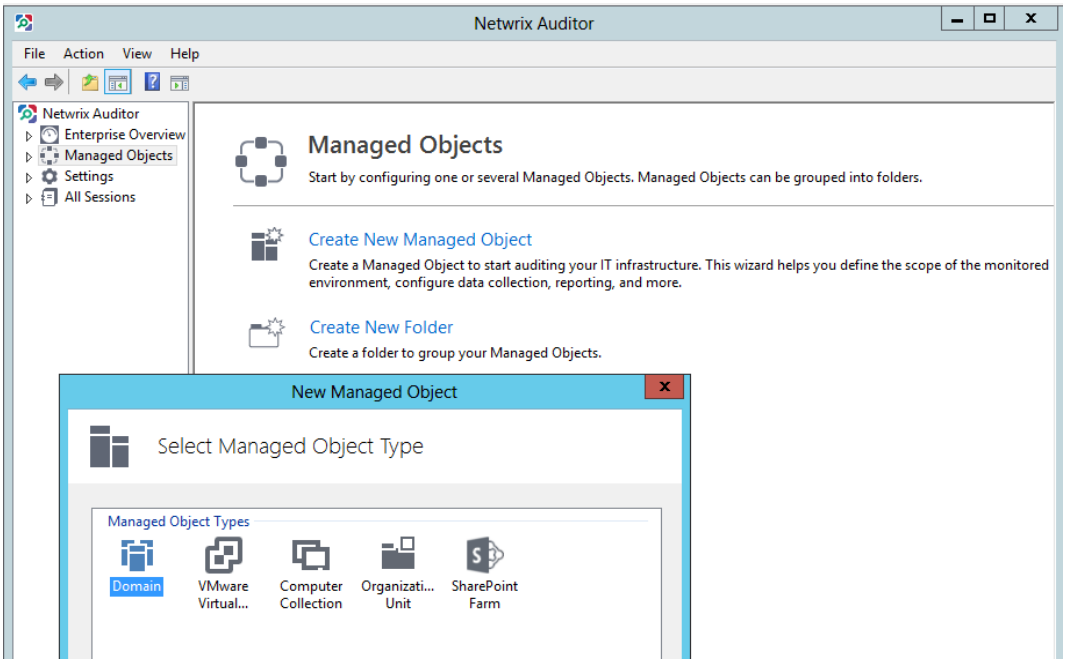
2.1.2. Create Managed Objects

To create a Managed Object, do one of the following:

- In the Netwrix Auditor console main window, select the system you want to audit. Some systems can be audited under several Managed Objects types (for example, Inactive User Tracking can be audited under Domain or Organizational Unit), so you will be prompted to select a Managed Object type.

- In the left pane, navigate to the **Managed Objects** node and select **Create New Managed Object**. In the **New Managed Object** wizard, select the Managed Object type. Some Managed Objects allow auditing several target systems (for example, under the Domain Managed Object you can audit Active Directory, Group Policy and Exchange Server). You will be prompted to select the systems you

want to audit on the further steps of the **New Managed Object** wizard.



Perform the following procedures to start auditing your IT Infrastructure:

- Create Managed Objects for Active Directory Auditing
- Create Managed Objects for Group Policy Auditing
- Create Managed Objects for Exchange Server Auditing
- Start Mailbox Access Auditing
- Create Managed Objects for Inactive User Tracking
- Create Managed Objects for Password Expiration Alerting
- Create Managed Objects for Windows File Server Auditing
- Start NetApp Filer Auditing
- Start EMC Storage Auditing
- Create Managed Objects for Event Log Management
- Create Managed Objects for SQL Server Auditing
- Create Managed Objects for Windows Server Auditing
- Create Managed Objects for User Activity Video Recording
- Create Managed Objects for VMware Auditing
- Create Managed Objects for SharePoint Auditing

2.1.3. Delete Managed Objects

1. In the left pane, navigate to your Managed Object under the **Managed Objects** node.
2. Right-click a Managed Object and select **Delete**.

2.1.4. Modify Managed Objects

Depending on the Managed Object type, your audited system and changes you want to apply, the modification procedures may vary. Perform the following procedures:

To...	Do...
To modify a list of systems that are audited within the Managed Object	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. In the right pane, click **Add / Remove Systems**. 3. In the **Edit Managed Object** wizard on the **Add / Remove Systems** step, select or clear check-boxes to add or remove systems. 4. Complete the wizard.
To modify settings, that affect a certain target system (for example, enable or disable audit, enable or disable **Lightweight Agents**, add emails to **Send Change Summary to** lists, modify delivery schedule, etc., modify auditing scope).	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. Expand your Managed Object and select a target system. 3. In the right pane, modify the settings. Depending on the target system, some settings are located in the right pane and can be modified there, while others are invoked as a pop-up dialog after clicking **Configure** next to **Advanced Options**. **NOTE:** For more information on available options and settings descriptions, refer to the Managed Objects creation procedures and Additional Options topics.
To change the Data Processing Account for the Managed Object	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. Right-click your Managed Object and select **Properties**. 3. Update the Data Processing Account. **NOTE:** The **Custom** account must be granted the same permissions and access rights as the default Data Processing Account. Refer to Netwrix Auditor Installation

To...	Do...
	and Configuration Guide for more information.
To modify the global settings (such as SMTP settings, Audit Archive location, Reports settings, licensing, default Data Processing Account, etc.)	1. In the left pane, navigate to **Settings**. 2. In the right pane, select a subnode depending on the changes required. 3. Apply new settings. See Configure Global Settings for more information.
To modify Active Directory / Group Policy / Exchange Server audit settings	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. Expand your Managed Object and select a target system. 3. In the right pane, select **Configure Audit** next to **Audit Configuration**.
To modify User Activity Video Recording auditing scope and recording settings	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. Expand your Managed Object and select **User Activity**. 3. In the right pane, do one of the following: • Click **Specify Users** next to **Users** to limit auditing to certain users. Create a list of users, specify exceptions if necessary. • Click **Specify Applications** next to **Applications** to limit auditing to certain applications. Create a list of applications, specify exceptions if necessary. • Click **Configure Video** next to **Video Recording Settings** to modify recording quality, durition and retention settings.

2.2. Create Managed Objects for Active Directory Auditing

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.

See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

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.
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.

Setting	Description
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. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

     NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

Setting	Description
SQL Server instance	Specify the name of an existing SQL Server instance where a

Setting	Description
	database for audit data will be created.
Windows Authentication	Select this option if you want to use the default Data Processing 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

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, you can 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 one of the following:
   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of the settings that are required for the product to function properly.

     If you select to configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

- **Manually**

  For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

9. On the **Specify <your_audited_system> Change Summary Recipients** step, click **Add** to specify emails where Change Summaries should be sent.

   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, enable or disable predefined Real-Time Alerts, or click **Add** to configure custom alerts. See Configure Real-Time Alerts for more information.

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.

2.3. Create Managed Objects for Group Policy Auditing

1. Do one of the following:

   - In the Netwrix Auditor console main window select **Group Policy**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Domain** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Group Policy** as the audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   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.
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. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.

5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

     NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

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 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

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 **Configure Audit in Target Environment** step, select one of the following:
   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of the settings that are required for the product to function properly.

     If you select to configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

     NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.
   - **Manually**

     For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
8. On the **Specify <your_audited_system> Change Summary Recipients** step, click **Add** to specify emails where Change Summaries should be sent.

   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.
9. 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.

2.4. Create Managed Objects for Exchange Server Auditing

1. Do one of the following:
   - In the Netwrix Auditor console main window select **Exchange Server**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Domain** as a Managed Object type in the **Create New Managed**

Object wizard. In this case you will prompted to select **Exchange Server** as the audited system later in the wizard.

See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

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.
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.

Setting	Description
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. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

     NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

Setting	Description
SQL Server instance	Specify the name of an existing SQL Server instance where a

Setting	Description
	database for audit data will be created.
Windows Authentication	Select this option if you want to use the default Data Processing 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

6. On the **Configure Audit in Target Environment** step, select one of the following:

   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of the settings that are required for the product to function properly.

     If you select to configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

     NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

   - **Manually**

     For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

7. On the **Specify <your_audited_system> Change Summary Recipients** step, click **Add** to specify

emails where Change Summaries should be sent.

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.

8. 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.

2.5. Start Mailbox Access Auditing

1. Do one of the following:
   - If you already have a Managed Object created for Exchange Server Auditing, navigate to this Managed Object in the Netwrix Auditor console, select **Exchange Server** system in the left pane, and click **Track Access** next to **Non-owner Mailbox Access Auditing** in the right pane.

     See Create Managed Objects for Exchange Server Auditing for more information.
   - If you do not want to create a Managed Object for Exchange Server Auditing, navigate to **Start** → **Programs** → **Netwrix Auditor** → **Netwrix Mailbox Access Auditing Tool**.
2. In the dialog that opens, specify the following settings and parameters. Click **Apply**. Review the following for additional information:

Option	Description
Enable	Make sure the **Enable** option is checked. **NOTE:** If later you disable the product by clearing this check-box, and then re-enable it after some time, data will start to be collected only after the first scheduled data collection task is run (at 3 AM by default). As a result, events that occur after the product is re-enabled and before the first scheduled task will not be reported. To avoid audit data loss, it is recommended to run a scheduled data collection task manually immediately after the product is re-enabled.
	Exchange Servers
Specify the Exchange servers you want to monitor	Click **Add** and enter the IP address or computer name, or import a list of monitored servers from a file. You can import a list of servers from a *.txt file containing one computer name or IP address per line. You can also remove computers you specified previously from the monitored servers list.

Option	Description
Use agents to collect detailed audit data	Select this check-box to enable agents that collect information required for detailed reports. **NOTE:** If this option is deselected, only summary reports will be available. If you choose not to use agents for audit data collection, you must configure native auditing on your monitored Exchange Servers. Refer to Netwrix Auditor Installation and Configuration Guide for more information.
	Reports
Report delivery schedule (daily at 3:00 AM by default)	Click **Modify** to configure the data processing and report delivery schedule. **NOTE:** To be able to configure this schedule, you must save your configuration first by clicking **Apply** at the bottom of the dialog.
Summary report	Select this report type to receive summary reports. These reports contain information on who accessed what mailbox and when.
Detailed report	Select this report type to receive detailed reports. These reports contain information on who accessed what mailbox and when, and what actions were performed on the accessed mailboxes' contents. **NOTE:** To receive detailed reports, the **Use agents to collect detailed audit data** option must be enabled.
Only report on mailboxes whose owners belong to these OUs	Select this check-box to filter data in reports by organizational units. Click **Select OUs** and specify a list of organizational units. Reports will include information only on non-owner access to mailboxes that belong to users from the specified OUs.
Attach reports as CSV files	Select this check-box to receive reports attached to emails as CSV files.
Report recipients	Enter the email addresses where reports must be delivered, separated by commas.
Notify users	Select this check-box if you want to notify users about non-owner access to their mailboxes.
Customize report template	Click **Customize** to edit the notification template, for example,

Option	Description
	modify the text of the message.
Notify only selected users	Select this check-box and click **Specify Users** to specify a list of users who will receive notifications on non-owner access to their mailboxes. Users not included in this list will not be notified.
	Report delivery settings
SMTP server name	Enter your SMTP server name.
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.
Authentication	Select this button to specify authentication settings.
Use 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.
Use 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.
	Audit Archive
Location	Click **Browse** to select the location for your Audit Archive. **NOTE:** If later you change the location of the Audit Archive, you will need to manually move the contents of this folder to the new location. Otherwise, the next data collection will be performed as the initial analysis, and events that occurred between the last data collection and the move of the audit

Option	Description
	archive will not be reflected in reports. Also, you will not be able to generate reports in the Report Viewer that involve data stored in the old location.
Enable long-term audit archiving for x months	Select this check-box to enable long-term archiving and specify how long collected audit data must be stored. **NOTE:** If this option is disabled, the product will only store information on non-owner access events that took place between the last two data collections.

3. In the **Scheduled Task Credentials** dialog, enter the default <domain_name\account_name> and password that will be used for data collection. To monitor several Exchange Servers in the domain where Netwrix Auditor is installed, specify the user that belongs to the **Domain Admins** group. To monitor Exchange Servers in different domains of the forest, specify the user that belongs to the **Enterprise Admins** group.

   NOTE: You will be prompted to specify the default account every time you save your current configuration.

4. Run the first data collection based on instructions provided in the dialog. The first data collection creates the initial snapshot of your monitored servers' current state. After the second data collection, which will take place at 3 AM the next day, you will receive a report on non-owner mailbox access.

2.6. Create Managed Objects for Password Expiration Alerting

1. Do one of the following:

   - In the Netwrix Auditor console main window select **Password Expiration Alerting**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Domain** or **Organizational Unit** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the

Specify Default Data Processing Account and **Configure Email Settings** steps of the wizard will be omitted.

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.
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	Select this check-box if your SMTP server requires SSL to be

Setting	Description
encrypted connection (SSL)	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. Depending on your Managed Object, on the **Specify Domain Name** or **Specify Organizational Unit Name** step, specify the target domain name or OU name in the FQDN format. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** option and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Configure Password Expiration Notifier Parameters** step, specify the following settings:

Parameters	Description
Send report to administrators	Enable this option and specify one or several email addresses for administrators to receive daily reports with a list of users whose accounts/passwords are going to expire in the specified number of days. Use period or semicolon to separate several addresses. **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.
Send report to the users' managers	Enable this option for reports to be delivered to the users' group managers. The managers are specified in the **Managed By** tab of the **AD users group Properties** dialog. **NOTE:** To edit the report template, click **Customize**.
List users whose accounts or passwords expire in <> days or less	Specify the expiration period for accounts and/or passwords to be included in the administrators and managers reports.
Notify users	Select the option to notify users that their passwords and/or accounts are about to expire.
Every day if their password expires in <> days or less	Select this option for users to be notified daily that their passwords are going to expire, and specify the number of days before the expiration date.

Parameters	Description
	NOTE: To edit the report template, click **Customize**.
First time when their password expires in <> days	Select this option for users to be notified three times, and specify the number of days before the expiration date for each of three notifications. **NOTE:** To edit the report template, click **Customize**.
Notify users by email every day if their account expires in	Select this option for users to be notified daily that their account is going to expire, and specify the number of days before the expiration date.
Filter users by organizational unit	To monitor users for expiring accounts/passwords that belong to certain organizational units within your Active Directory domain, select this option and click **Select OUs**. In the dialog that opens, specify the OUs that you want to monitor. Only users belonging to these OUs will be notified and included in the administrators and managers reports.
Filter users by group	To monitor users for expiring accounts/passwords that belong to certain groups within your Active Directory domain, select this option and click the Select OUs button. In the dialog that opens, specify the groups that you want to monitor. Only users belonging to these groups will be notified and included in the administrators and managers reports.

6. 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.

2.7. Create Managed Objects for Inactive User Tracking

1. Do one of the following:
   - In the Netwrix Auditor console main window select **Inactive User Tracking**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Domain** or **Organizational Unit** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

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.
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.

Setting	Description
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. Depending on your Managed Object, on the **Specify Domain Name** or **Specify Organizational Unit Name** step, specify the target domain name or OU name in the FQDN format. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Configure Inactive User Tracker** step, specify the following settings:

Parameters	Description
Consider user inactive after	Specify account inactivity period, after which a user is considered to be inactive.
Notify manager after	Specify account inactivity period, after which the account owner's manager must be notified.
Set random password after	Specify account inactivity period, after which a random password will be set for this account.
Disable account after	Specify account inactivity period, after which the account will be disabled.
Move to a specific OU after	Specify account inactivity period, after which the account will be moved to a specified organizational unit.
Delete accounts after	Specify account inactivity period, after which the account will be deleted.
Process user accounts	Select this check-box to track user accounts activity.
Process computer accounts	Select this check-box to track computer accounts activity.
Send report to	Enter the email addresses of daily report recipients. Emails on errors during data collection will also be delivered to these recipients.

Parameters	Description
	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.

6. 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.

2.8. Create Managed Objects for Windows Server Auditing

1. Do one of the following:
   - In the Netwrix Auditor console main window select **Windows Server**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   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.
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 Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

  NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

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 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

6. On the **Add Items to Computer Collection** step, select items that you want to audit. You can add

several items to collection. Click **Add** 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 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**. • Exclude the computers you do not want to audit. To do this, click **Exclude** to specify a container with the computers you do not want to audit. **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.
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 on every data collection. If you select the **Import on every data collection** option, you can later modify the list of your monitored computers by editing the .txt file. The audited computers list will be updated on the next data collection.

7. On the **Select Data Collection Method** step, you can 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 one of the following:

- **Automatically for the selected audited systems**

  Click the arrow button next to an audited system to expand the list of the settings that are required for the product to function properly.

  If you select to configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

  NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

- **Manually**

  For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

9. On the **Select Monitored Systems Components** step, select the system components that you want to audit for changes.
10. On the **Windows Server Change Reporter Change Summary Delivery** step, specify the reports recipients.
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.

2.9. Create Managed Objects for Event Log Management

1. Do one of the following:

   - In the Netwrix Auditor console main window select **Event Log**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

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.
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 Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

     NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

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 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.

Setting	Description
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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

6. On the **Add Items to Computer Collection** step, select items that you want to audit. You can add several items to collection. Click **Add** and select one of the predefined platform types: **Windows Server** or **Syslog-based Platform.**

   NOTE: If you have configured custom syslog platforms previously, they will appear in the **Syslog-based Platforms list**.

   Depending on the platform type selected, specify the object to be monitored. Review the following for additional information:

Option	Description
Computer name / Single computer or device	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 (Available for **Windows Server** platform only)	Allows specifying a whole AD container. Click **Browse** to select from the list of containers in your network. You can also: • Select a particular computer type to be monitored within the chosen AD container: **Domain controllers, Servers (excluding domain controllers)**, or **Workstations**. • Exclude the computers you do not want to monitor. To do it, click **Exclude** to specify a container with the computers you do not want to monitor. **NOTE:** The list of containers does not include child domains of trusted domains. If the product is installed on a computer running Windows XP / Windows Server 2003, trusted domains will also not appear in the list of AD containers. Use other options **(Computer name, IP address range**, or

Option	Description
	Import computer names from a file) to specify the target computers.
IP address range / Computers within an IP 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 / Import servers or devices list	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 on every data collection. If you select the Import on every data collection option, you can later modify the list of your monitored computers by editing the .txt file. The audited computers list will be updated on the next data collection.

7. On the **Select Data Collection Method** step, you can 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 **Specify <your_audited_system> Change Summary Recipients** step, click **Add** to specify emails where Change Summaries should be sent.

   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.
9. On the **Configure Real-Time Alerts** step, enable or disable predefined Real-Time Alerts, or click **Add** to configure custom alerts. See Configure Real-Time Alerts for more information.
10. On the **Configure Audit Archiving Filters** step, enable or disable predefined filters, or click **Add** to configure custom filters. See Configure Audit Archiving Filters for more information.
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.

2.10. Create Managed Objects for Windows File Server Auditing

1. Do one of the following:
   - In the Netwrix Auditor console main window select **File Servers**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **File Servers** as the audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   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 Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

     NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to

monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

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 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

6. On the **Add Items to Computer Collection** step, click **Add** to select items that you want to audit. You can add several items to collection.

NOTE: Netwrix Auditor supports audit of DFS and clustered file servers. Refer to the following Knowledge Base articles: Does Netwrix Auditor support DFS? and How to configure Netwrix Auditor to audit a clustered file server? for more information.

In the dialog that opens, select the item type and add / browse for a computer name or add / browse for a new shared object.

- **Windows File Share**—Provide a path to a shared resource.
- **Windows Server**— 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 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**. • Exclude the computers you do not want to audit. To do this, click **Exclude** to specify a container with the computers you do not want to audit. **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.
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 on every data collection. If you select the **Import on every data collection** option, you can later modify the list of your monitored computers by editing the .txt file. The audited computers list will be updated on the next data collection.

7. On the **Configure File Server Change Reporter Settings** step, specify the reports recipients. Click **Advanced** to configure advanced settings if necessary. Review the following for additional information:

Option	Description
Enable network traffic compression	The network traffic compression option is recommended for slow connections and distributed multi-site networks. When enabled, a lightweight agent is executed remotely on each file server to collect and compress audit data before transfer. This results in almost 100 times less data transferred with minimal impact on target computers' performance.
Enable large server support	This option is recommended to speed up data collection from file servers storing a large amount of data (500 000 and more files).
File Version Control	See Roll Back Changes With Windows File Server Auditing for more information.
Attach the email reports as a CSV file	Select this option to receive reports as attachments. Otherwise, you will receive reports as a part of the email body.

8. 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.

2.11. Start NetApp Filer Auditing

1. On computer where Netwrix Auditor resides, navigate to *%Netwrix Auditor installation folder%/File Server Change Reporter* and select **File Server Change Reporter (Standard Edition)**.
2. Check **Enable File Server Change Reporter**.
3. Click **Add** next to the **UNC Path** list. In the **Add UNC Path** dialog, complete the following fields:
   - Specify the folder you want to audit. You can specify a file server name to audit all shares located on that server or UNC path to a folder or share you want to audit.
   - Select **NetApp Filer** as a file server platform. Click **Configure** and provide credentials to the NetApp server web interface and path to the event log.
   - Check the types of access you want to monitor.

   You can also **Import** a *.txt file containing a list of UNC paths to the file servers, one entry per line.
4. In **Store data to** specify the path, where the snapshots will be saved.
5. You can set **Enable long-term achieving for** <n> months. By default, collected data is stored for two days. Select **Enable long-term archiving for** if you need to keep data for longer periods of time. It affects only the local repository and not the SQL database.
6. **Enable network traffic compression** is not available for NetApp Filer appliances since they are not Windows-based.

7. Select **Enable large server support** to speed up processing of file servers with a large number of files (500 000 and more).
8. **File Version Control** is not available for NetApp Filer appliances, since they are not Windows-based while this options requires native **Windows Volume Shadow Copying** feature.
9. Select **Attach the email reports as a CSV file**. Otherwise, you will receive reports as a part of the email body.
10. Click **Configure** next to **Advanced reporting (SQL SRS)**. Complete the **Reports Configuration** wizard. You can install new SQL Server instance or use an existing one. Complete the following fields:

Parameter	Description
Server name	Specify SQL Server instance to store database with collected audit data.
Database	Specify database to store collected audit data.
User name	Specify a user name for the SQL Server authentication. This user must be granted **database owner (dbo)** role. Refer to Netwrix Auditor Installation and Configuration Guide for more information.
Password	Enter a password for the SQL Server authentication.
Windows Authentication	Select this option if you want to use the Data Processing Account.
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.

11. Specify **Email report delivery settings**.

NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the email settings on their configuration, the fields under **Email report delivery settings** will be prepopulated with this data.

Complete the following fields:

Parameter	Description
Report on modifications	Enter the email address where the reports on file modifications must be delivered. These reports are based on the **Successful modifications** events.

Parameter	Description
Report on reads	Enter the email address where the reports on the read file access or failed read attempts must be delivered. These reports are based on the **Successful reads** and/or **Failed read attempts** events.
SMTP server	Enter your SMTP server name.
Port	Specify your SMTP server port number.
From address	Enter the address that will appear in the "From" field in the reports. 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.

12. Click **Advanced** next to **Additional product configuration** to configure SMTP settings. Complete the following fields:

Parameter	Description
Report delivery schedule	By default, reports are generated and delivered at 3.00 AM every day. Click **Change**. In the dialog that opens, click **New** and specify the delivery schedule.
SMTP authentication	Select this check-box if your mail server requires the SMTP authentication.
Username	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Use SSL	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.

13. Click **Start** to launch the Netwrix Auditor console.
14. Click **Apply**.
15. In the **Scheduled Task Credentials** dialog specify the Data Processing Account (in the *domain_name\account_name* format) to run the scheduled task.

NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account on their configuration, the account will prepopulated with this data.

This account must have at least the following rights:

- **Local administrator** 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 the **database owner (dbo)** role.
- **Log on as a batch job** policy defined for this account.

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.

2.12. Start EMC Storage Auditing

1. On computer where Netwrix Auditor resides, navigate to *%Netwrix Auditor installation folder%/File Server Change Reporter* and select **File Server Change Reporter (Standard Edition)**.
2. Check **Enable File Server Change Reporter**.
3. Click **Add** next to the **UNC Path** list. In the **Add UNC Path** dialog, complete the following fields:
   - Specify the folder you want to audit. You can specify a file server name to audit all shares located on that server or UNC path to a folder or share you want to audit.
   - Select **EMC VNX / VNXe / Celerra** as a file server platform.
   - Check the types of access you want to monitor.

   You can also **Import** a *.txt file containing a list of UNC paths to the file servers, one entry per line.
4. In **Store data to** specify the path, where the snapshots will be saved.
5. You can set **Enable long-term achieving for** <n> months. By default, collected data is stored for two days. Select **Enable long-term archiving for** if you need to keep data for longer periods of time. It affects only the local repository and not the SQL database.
6. **Enable network traffic compression** is not available for EMC VNX / VNXe / Celerra appliances since they are not Windows-based.
7. Select **Enable large server support** to speed up processing of file servers with a large number of files (500 000 and more).
8. **File Version Control** is not available for EMC VNX / VNXe / Celerra appliances, since they are not Windows-based while this options requires native **Windows Volume Shadow Copying** feature.
9. Select **Attach the email reports as a CSV file**. Otherwise, you will receive reports as a part of the email body.
10. Click **Configure** next to **Advanced reporting (SQL SRS)**. Complete the **Reports Configuration**

wizard. You can install new SQL Server instance or use an existing one. Complete the following fields:

Parameter	Description
Server name	Specify SQL Server instance to store database with collected audit data.
Database	Specify database to store collected audit data.
User name	Specify a user name for the SQL Server authentication. This user must be granted **database owner (dbo)** role. Refer to Netwrix Auditor Installation and Configuration Guide for more information.
Password	Enter a password for the SQL Server authentication.
Windows Authentication	Select this option if you want to use the Data Processing Account.
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.

11. Specify **Email report delivery settings**.

NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the email settings on their configuration, the fields under **Email report delivery settings** will be prepopulated with this data.

Complete the following fields:

Parameter	Description
Report on modifications	Enter the email address where the reports on file modifications must be delivered. These reports are based on the **Successful modifications** and/or **Failed modification attempts** events.
Report on reads	Enter the email address where the reports on the read file access or failed read attempts must be delivered. These reports are based on the **Successful reads** and/or **Failed read attempts** events.
SMTP server	Enter your SMTP server name.
Port	Specify your SMTP server port number.
From address	Enter the address that will appear in the "From" field in the reports.

Parameter	Description
	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.

12. Click **Advanced** next to **Additional product configuration** to configure SMTP settings. Complete the following fields:

Parameter	Description
Report delivery schedule	By default, reports are generated and delivered at 3.00 AM every day. Click **Change**. In the dialog that opens, click **New** and specify the delivery schedule.
SMTP authentication	Select this check-box if your mail server requires the SMTP authentication.
Username	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Use SSL	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.

13. Click **Start** to launch the Netwrix Auditor console.
14. Click **Apply**.
15. In the **Scheduled Task Credentials** dialog specify the Data Processing Account (in the *domain_name\account_name* format) to run the scheduled task.

NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account on their configuration, the account will prepopulated with this data.

This account must have at least the following rights:

- **Local administrator** 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 the **database owner (dbo)** role.
- **Log on as a batch job** policy defined for this account.

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.

2.13. Create Managed Objects for User Activity Video Recording

1. Do one of the following:
   - In the Netwrix Auditor console main window select **User Activity**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   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.
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 Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

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 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

6. On the **Add Items to Computer Collection** step, select items that you want to audit. You can add several items to collection. Click **Add** and define the items. 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 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**. • Exclude the computers you do not want to audit. To do this, click **Exclude** to specify a container with the computers you do not want to audit. **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.
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 on every data collection. If you select the **Import on every data collection** option, you can later modify the list of your monitored computers by editing the .txt file. The audited computers list will be updated on the next data collection.

7. On the **Specify Users** step, select the users whose activity should be recorded. You can select **All users** or create a list of **Specific users**. Certain users can also be added to **Exceptions** list.
8. On the **User Activity Video Reporter Activity Summary Delivery** step, set the delivery schedule and click **Add** to specify emails where Activity Summaries should be sent to.

   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.
9. 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.

2.14. Create Managed Objects for SQL Server Auditing

1. Do one of the following:
   - In the Netwrix Auditor console main window select **SQL Server**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **SQL Server** as the audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   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 Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

     NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to

monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

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 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

6. On the **Add Items to Computer Collection** step, select items that you want to audit. Click **Add** and add / browse for a server. You can add several servers to collection.
7. On the **Configure SQL Server Change Reporter Settings** step, specify recipients of the SQL Server configuration change summaries. To monitor database content, select **Enable database content audit** and add recipients.

   Database Content Audit allows setting rules for the data to be monitored and therefore to receive change reports on the selected data only. Click **Specify** to open the **Database Content Audit** dialog.

In the **Database Content Audit** dialog, click **Add** to create columns monitoring rules and set the number of data changes per SQL transaction to be included in reports.

NOTE: The following column types are currently not supported: `text, ntext, image, binary, varbinary, timestamp, sql_variant`.

You can also configure the format of reports sent by email. Click **Configure** to edit the settings. In the **Change Summary Format** dialog that opens, the following options are available:

- **Attach as a CSV file**—If selected, the change summary report will be sent as a file attached to an email. Otherwise, you will receive the report as a part of the email body.
- **Compress before sending**—If selected, the attached file will be sent in the compressed format.

8. 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.

2.15. Create Managed Objects for VMware Auditing

1. Do one of the following:
   - In the Netwrix Auditor console main window select **VMware**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **VMware Virtual Center** as a Managed Object type in the **Create New Managed Object** wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   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.
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 VMware Virtual Center Name** step, specify the VMware Center URL. If you want to use a specific account to access data from your virtual machines (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

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.

  NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

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 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom

Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

6. On the **Recipients of VMware Change Reporter Email Reports** step, click **Add** to specify emails where audit reports should be sent.

   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.

   In the **VMware Credentials** section, you should also specify user name and password to be used when connecting to VMware instance.

7. 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.

2.16. Create Managed Objects for SharePoint Auditing

1. Do one of the following:

   - In the Netwrix Auditor console main window select **SharePoint**.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **SharePoint Farm** as a Managed Object type in the **Create New Managed Object** wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other target systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   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 have 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 the **database owner (dbo_owner)** role.
   - Must have the **Log on as a service** policy defined. The **Log on as a service** 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 service** policy defined locally or on the domain level, the local **Log on as a service** policy will be reset. 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.
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 SharePoint Farm** step, enter the SharePoint Central Administration website URL. If you want to use a specific account to access data from this SharePoint Farm (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.

NOTE: Netwrix Auditor cannot verify the Central Administration URL address if your Data Processing Account does not belong to the **Farm Administrators** group on your SharePoint Central Administration site. It does not affect the product operability, you can proceed with the Managed Object creation.

5. On the **Reports Settings** step, select **Enable Reports** if you want to use the SSRS-based Reports. Otherwise audit data will not be written to a SQL database.

   NOTE: You can skip this step now and enable and configure reports later. See Configure Reports for more information.

   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.

     NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the product configuration. See Install Microsoft SQL Server for more information.

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 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.

If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable Reports feature. If you want to use custom Reports settings for this Managed Object (e.g. write data to a different SQL database), you can change the Reports settings later. See Configure Reports for more information.

6. On the **Configure Audit in Target Environment** step, select one of the following:

   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of the settings that are required for the product to function properly.

     If you select to configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

     NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

   - **Manually**

     For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

7. On the **Select SharePoint Auditing Scope** step, you select the type of changes you want to track and the scope of objects that will be audited in addition to Central Administration auditing.

   Netwrix Auditor allows auditing the entire SharePoint farm. Alternatively, you can limit the auditing scope to separate web applications and site collections. To do it, select **Specified SharePoint objects** and click **Specify**. In the **Specify SharePoint Objects** dialog, do one of the following:

   - Click **Add** and provide URL to web application or site collection.
   - Click **Import** and browse for a file that contains a list of web applications or site collections.

   NOTE: Netwrix Auditor ignores changes to system data (for example, hidden and system lists or items are not audited). Netwrix Auditor also ignores the content changes to sites and objects on the site collections located on Central Administration web application, but the security changes that occurred there are tracked and reported anyway.

8. On the **SharePoint Change Summary Delivery** step, click **Add** to specify emails where the Change Summaries should be sent. By default, the emails are generated at 3 AM, modify the schedule if necessary.

   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.

9. On the **Deploy Netwrix Auditor Agent for SharePoint** step, specify the agent deployment method. Select one of the following:

- **Automatically**—The installation will run under the Data Processing Account on the New Managed Object wizard completion.

  Prior to agent installation, review the following prerequisites and apply the required settings if necessary:

  - The agent must be deployed to the computer where SharePoint Central Administration is installed.
  - The **SharePoint Administration (SPAdminV4)** service must be started on this computer. Refer to Netwrix Auditor Installation and Configuration Guide for more information.
  - To run the agent installation, the user must be granted the following rights and permissions:
    - Must be a member of the **local Administrators** group on SharePoint server, where the agent will be deployed.
    - Must be granted the **SharePoint_Shell_Access** role on SharePoint SQL Server configuration database. Refer to Netwrix Auditor Installation and Configuration Guide for more information.
- **Manually**—Refer to Netwrix Auditor Installation and Configuration Guide for more information.

NOTE: During the agent installation / uninstallation your SharePoint sites may be unavailable.

10. 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.

3. Data Collection

This chapter explains the Netwrix Auditor data collection workflow, provides a Change Summary example and instructions on how to modify the default Change Summary delivery settings, and explains how to check data collection status via the Sessions interface.

For more information see:

- Data Collection Workflow
- Change Summary
- Sessions

3.1. Data Collection Workflow

The Netwrix Auditor data collection workflow is as follows:

1. When a new Managed Object is created, Netwrix Auditor starts collecting audit data from the managed Active Directory domain or organizational unit, computer collection, VMware Virtual Center, or a SharePoint farm. 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 the specified recipients stating that the initial analysis has completed successfully. If you do not want to wait until a scheduled data collection, you can launch it manually. See To launch data collection manually for more information.

   Each data collection, both scheduled or launched manually, is referred to as a 'session'. You can review sessions in the Netwrix Auditor console to check if a data collection completed successfully, or with errors/warnings. See Sessions for more information.

   NOTE: The following Netwrix Auditor features employ a different data collection method:

   - User Activity Video Recording
   - SharePoint Auditing.

   Instead of using a scheduled task for data collection, they require an agent to be installed on the monitored computers / SharePoint server. The rest of the workflow is applicable to these features.

2. If during a data collection a change or an event is detected that triggers an alert, an email notification is sent immediately to the specified recipients. The Real-Time Alerts functionality is currently supported by the following Netwrix Auditor features:

   - Active Directory Auditing
   - Event Log Management

Refer to Configure Real-Time Alerts for detailed instructions on how to use predefined and create custom alerts.

3. Once a day (at 3:00 AM by default), Netwrix Auditor writes collected audit data to a local file-based storage: Audit Archive.
4. If the Reports functionality is enabled and configured, audit data is then imported from the Audit Archive to a SQL database. Refer to Configure Reports for detailed instructions on how to configure SSRS-based Reports.
5. If the State-in-Time Reports functionality is enabled, Netwrix Auditor also makes a point-in-time snapshot of the monitored system's current state and writes it to the Audit Archive. The State-in-Time Reports functionality is currently supported by the following Netwrix Auditor features:
   - Active Directory Auditing
   - Group Policy Auditing

   Refer to State-in-Time Reports for detailed instructions on how to configure and use the State-in-Time Reports functionality.
6. At the same time, Netwrix Auditor generates a Change Summary and emails it to the specified recipients. Refer to Refer to Change Summary for detailed instructions on

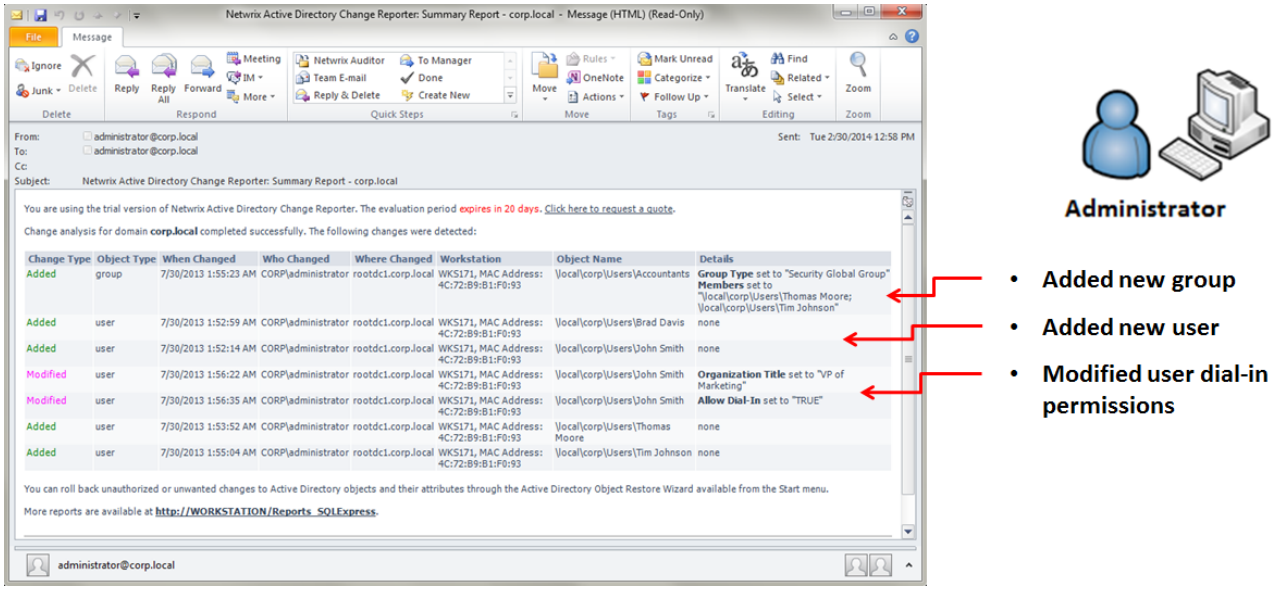
To launch data collection manually

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **your_Managed_Object_name** .
2. Select the audited system for which you want to run a data collection, and click **Run**.

NOTE: Depending on the size of the monitored environment and the number of changes, data collection may take quite long.

3.2. Change Summary

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:



The example Change Summary provides the following information:

Parameter	Description
Change Type	Shows the type of action that was performed on an AD object: • Added • Removed • Modified
Object Type	Shows the type of the modified AD 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.
Workstation	Shows the name / IP address of the computer where the user was logged on when they made the change.
Object Name	Shows the path to the modified AD object.
Details	Shows the before and after values of the modified AD object.

NOTE: The Change Summary example above applies to the Active Directory Auditing feature. Other Change Summaries generated and delivered by Netwrix Auditor may vary slightly depending on the audited system or application.

Refer to the following procedures for instructions on how to modify the default Change Summary delivery schedule, initiate an on-demand Change Summary delivery and view changes for a specified date range:

- To modify Change Summary delivery schedule
- To initiate on-demand Change Summary delivery
- To generate a Change Summary for a specified date range

To modify Change Summary delivery schedule

To modify the Change Summary generation and delivery schedule, follow the instructions in the table below depending on the Netwrix Auditor feature:

Feature	Instructions
Active Directory Auditing Group Policy Auditing Exchange Server Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Active Directory**. 2. In the right pane, modify the Change Summary delivery time and interval.
Event Log Management	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Event Log**. 2. In the right pane, modify the daily Events Summary time.
User Activity Video Recording	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **User Activity**. 2. In the right pane, click **Configure Delivery** in the **Activity Summary Delivery** section and modify the Activity Summary delivery time and interval.
Windows Server Auditing	1. In the Windows Task Scheduler Library, locate the **Netwrix Management Console - Windows Server Change Reporter - <Managed Object name>** task. 2. Right-click the task and select Properties from the pop-up menu. In the dialog that opens, navigate to the Triggers tab and click New. 3. Modify the task schedule and click OK to save the changes.
Windows File Server Auditing EMC Storage Audting NetApp Filer Auditing	1. In the Windows Task Scheduler Library, locate the **Netwrix Management Console - File Server Change Reporter - <Managed Object name>** task. 2. Right-click the task and select **Properties** from the pop-up menu. In the dialog that opens, navigate to the **Triggers** tab and click **New**. 3. Modify the task schedule and click **OK** to save the changes.

Feature	Instructions
SQL Server Auditing	1. In the Windows Task Scheduler Library, locate the **Netwrix Management Console - SQL Server Change Reporter - <Managed Object name>** task. 2. Right-click the task and select **Properties** from the pop-up menu. In the dialog that opens, navigate to the **Triggers** tab and click **New**. 3. Modify the task schedule and click **OK** to save the changes.
VMware Auditing	1. In the Windows Task Scheduler Library, locate the **Netwrix Management Console - VMware Infrastructure 3 Changes - <Managed Object name>** task. 2. Right-click the task and select **Properties** from the pop-up menu. In the dialog that opens, navigate to the **Triggers** tab and click **New**. 3. Modify the task schedule and click **OK** to save the changes.
SharePoint Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **SharePoint**. 2. In the right pane, click **Configure Delivery** in the **Change Summary Delivery** section and modify the Change Summary delivery time and interval.
Mailbox Access Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Exchange Server**. 2. In the right pane, click **Track Access** in the **Non-owner Mailbox Access Auditing** section. 3. In the dialog that opens, click Modify in the **Reports** section and edit the default Change Summary schedule. 4. Click **Apply** in to save the changes.
Password Expiration Alerting	The Password Expiration Alerting feature does not provide the Change Summary functionality. For instructions on how to configure user notifications and administrator and manager reports, refer to Create Managed Objects for Password Expiration Alerting
Inactive User Tracking	The Inactive User Tracking feature does not provide the Change Summary functionality. For instructions on how to configure manager notifications, refer to Create Managed Objects for Inactive User Tracking

To initiate on-demand Change Summary delivery

If you do not want to wait until a scheduled delivery, you can launch data collection manually. When the data collection task has completed, a Change Summary will be generated and sent to the specified recipients. It will list all changes that occurred since the last scheduled or on-demand Change Summary delivery. Follow the instructions in the table below depending on the Netwrix Auditor feature:

Feature	Instructions
Active Directory Auditing Group Policy Auditing Exchange Server Auditing Event Log Management Windows Server Auditing Windows File Server Auditing SQL Server Auditing VMware Auditing SharePoint Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>**. 2. In the right pane, click **Run**. A Change Summary will be generated and sent to the specified recipients.
Mailbox Access Auditing	1. In the Windows Task Scheduler Library, locate the **Netwrix Non-owner Mailbox Access Reporter for Exchange>** task. 2. Right-click the task and select **Run** from the pop-up menu. A Change Summary will be generated and sent to the specified recipients.
User Activity Video Recording	This functionality is not supported by the User Activity Video Recording feature.

NOTE: Depending on the size of the audited environment and the number of changes, Change Summary generation may take quite long.

To generate a Change Summary for a specified date range

You can generate an HTML Change Summary for a specific data range. The Change Summary will be displayed in your default web browser. Follow the instructions in the table below depending on the Netwrix Auditor feature:

Feature	Instructions
Active Directory Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Active Directory**.

Feature	Instructions
	2. In the right pane, click **Generate Summary** in the **Change Viewer** section. 3. Select the audited system and the date range and click **Generate Summary**.
Group Policy Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Group Policy**. 2. In the right pane, click **Generate Summary** in the **Change Viewer** section. 3. Select the audited system and the date range and click **Generate Summary**.
Exchange Server Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Exchange Server**. 2. In the right pane, click **Generate Summary** in the **Change Viewer** section. 3. Select the audited system and the date range and click **Generate Summary**.
Event Log Management	1. In the product installation directory, navigate to \Netwrix\Event Log Manager. Locate a file called Viewer and double-click to launch it. 2. Select the Managed Object name, the computer for which you want to generate an Events Summary, the target event log, and the date range. Click **View**.
Windows Server Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → Windows Servers. 2. In the right pane, click **Generate Summary** next to **Change Viewer**. 3. Select the server for which you want to generate a Change Summary and the date range, and click **Generate Summary**.
Windows File Server Auditing	1. In the product installation directory, navigate to *\Netwrix\File Server Change Reporter*. Locate a file called Report Viewer and double-click to launch it. 2. Select the server for which you want to generate a Change Summary, the type of data you want to include, and the date

Feature	Instructions
	range. Click **Generate**.
SQL Server Auditing	1. In the product installation directory, navigate to *\Netwrix\SQL Server Change Reporter*. Locate a file called Report Viewer and double-click to launch it. 2. Select the server for which you want to generate a Change Summary, the type of data you want to include, and the date range. Click **Generate**.
VMware Auditing	1. In the product installation directory, navigate to *\Netwrix\Change Reporter for VI3 Full Version*. Locate a file called Report Viewer and double-click to launch it. 2. Select the server for which you want to generate a Change Summary and the date range and click **Generate**.
SharePoint Auditing	This functionality is not supported by the SharePoint Auditing feature.
Mailbox Access Auditing	1. In the product installation directory, navigate to *\Netwrix\Non-owner Mailbox Access Reporter for Exchange*. Locate a file called Report Viewer and double-click to launch it. 2. Select the server for which you want to generate a Change Summary, the date range, the filters and the type of report. Click **Export**.
User Activity Video Recording	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **User Activity** → Activity Records. 2. Specify the date range and the filters and click **Generate Summary**.

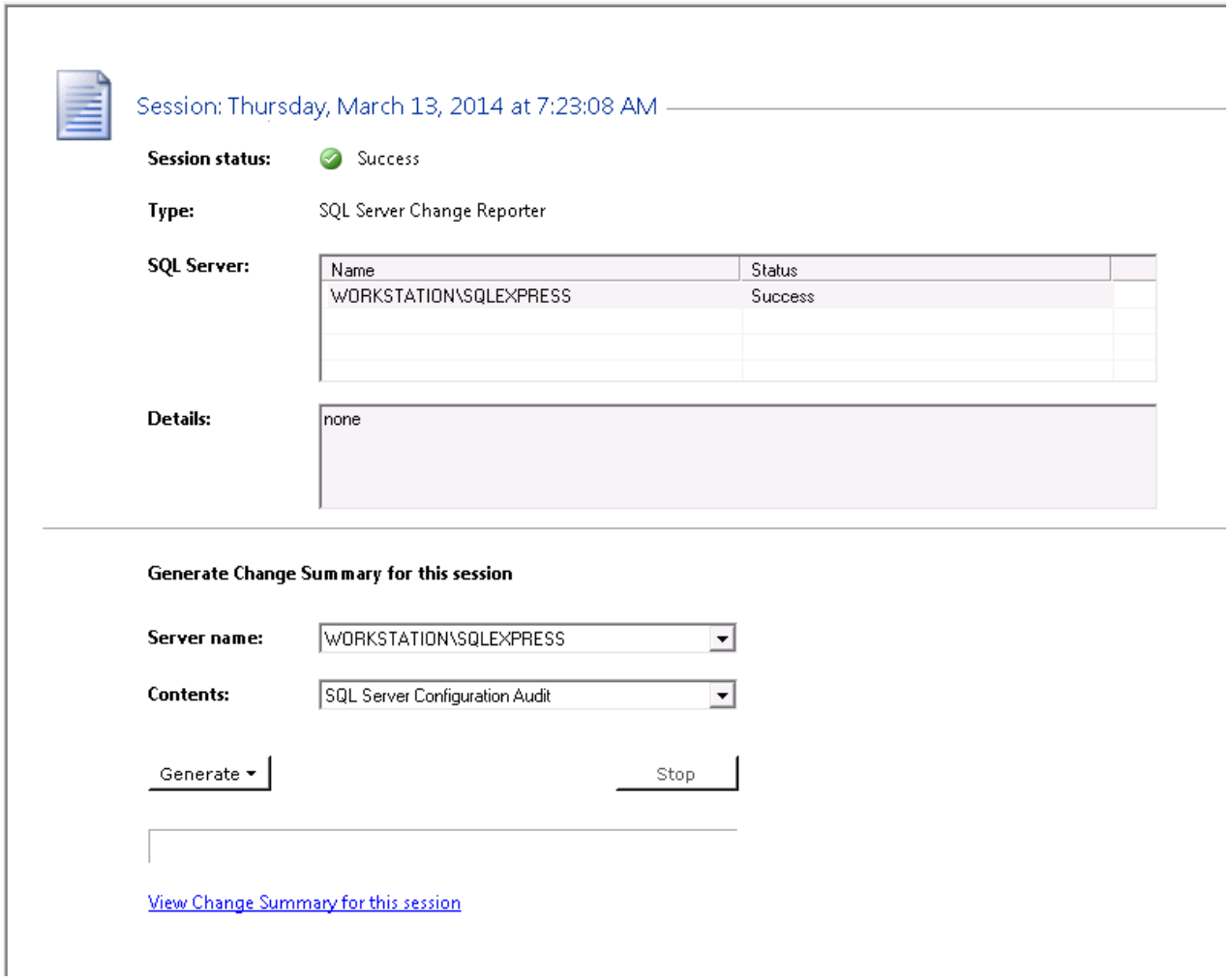
3.3. Sessions

In Netwrix Auditor, a session is a scheduled or an on-demand data collection that triggers Change Summary generation and delivery. You can review session results for

- an individual Netwrix Auditor feature under an individual Managed Object: in the Netwrix Auditor console navigate to **Managed Object** → **your_Managed_Object** → **audited_system** → **Sessions**.
- in bulk for all Managed Objects and all audited systems: in the Netwrix Auditor console navigate to **All Sessions**.

NOTE: Sessions are not available for the User Activity Video Recording and the SharePoint Auditing features, as they do not use a scheduled task for data collection.

When you select a Session, its details are displayed in the right pane:



Session status can be 'Success'. 'Warning', 'Error' and 'Fatal Error'. If a data collection completed with warnings or errors, they will be listed in the Details field.

You can generate a Change Summary for a particular session by clicking **Generate**.

You can limit the number of sessions available for review in the Netwrix Auditor console by specifying their retention period. See Configure Audit Archive Settings for more information.

4. Reports

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.).

If your situation requires the use of additional reports, you can order custom report templates from Netwrix.

In Netwrix Auditor, the following types of reports are available:

- **Dashboards**: provide quick access to important statistics across the audited IT infrastructure. They allow you to see the activity trends by date, user, server or audited IT system, and drill through to detailed reports for further analysis. The Enterprise Overview dashboard aggregates the information on changes from all audited systems and provides a centralized overview. System-specific dashboards reflect all changes across all Managed Objects where audit of this target system is enabled. See Dashboards for more information.
- **Enterprise Overview reports**: aggregate data from all audited systems and all Managed Objects. Enterprise-wide reports list all changes that occurred across the audited IT infrastructure. System-specific reports aggregate data from all Managed Objects where audit of this target system is enabled. See Enterprise-Wide Reports for more information.
- **Overview reports**: system-specific reports that aggregate audit data for an individual Managed Object. They provide a high-level overview of changes within a selected time period. Overview reports consist of four charts, showing the activity trends by date, user, object type or server, and drill through to detailed table reports for further analysis. See Overview Reports for more information.
- **Change reports**: system-specific reports that aggregate audit data for an individual Managed Object. Change reports show detailed data on changes and provide grouping, sorting and filtering capabilities. Each change report has a different set of filters allowing you to manage the collected data in the most convenient way. See Change Reports for more information.
- **State-in-time reports**: system-specific reports that aggregate data for an individual Managed Object and allow reviewing the point-in-time state of the audited system. These reports are based on daily snapshots and help you paint a picture of your system's configuration at a specific moment in time. See State-in-Time Reports for more information.
- **Reports with extended audit data**: system-specific reports that aggregate data for an individual Managed Object and provide additional audit details, such as the name of the originating workstation, i.e. the computer where the user was logged on when they made the change, and the possibility to filter audit data by Active Directory group membership, which means you can get data on changes performed by members of specific groups only. See Reports with Extended Audit Data for more information.

- **Change Review History**: system-specific reports that aggregate data for an individual Managed Object and can be used as a tool in the basic change management process. These reports allow setting s a review status for each change and providing comments. See Change Review History Reports for more information.
- **Changes with Video**: system specific reports that aggregate all changes for an individual Managed Object a provide a link to a video file showing *how* each change was made. This functionality requires the User Activity Video Recording feature to be configured. See Reports with Video for more information.

Reports can be viewed in the Netwrix Auditor console, or in a web browser.

To view reports in the Netwrix Auditor console

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **audited_system** → **Reports**.
2. Select a report from one of the folders. The report filters will be displayed on the right.
3. Specify filter values and click **View Report** (**View Chart** for chart reports). The report will be generated and displayed in the right pane.

To view reports in a web browser

1. Open a web browser and type the Report Manager URL (it can be found in the Netwrix Auditor console, under **Settings** → **Reports**).
2. In the page that opens, navigate to the report you want to generate and click the report name. The report will be displayed showing the changes that occurred in the last 24 hours. You can modify the report filters and click **View Report** to apply them.

4.1. Configure Reports

To configure SSRS-based Reports, or to modify the Reports settings for your Managed Objects, perform the following procedures:

- To specify SQL Server settings
- To upload reports to the Report Server
- To assign permissions to view reports
- To configure database retention policy
- To import audit data to a SQL database

To specify SQL Server settings

NOTE: You only need to perform this procedure if you did not enable the Reports functionality on Managed Object creation and decide to enable it later, or if you want to modify the Reports

settings for an individual Managed Object. For instructions on how to configure and modify the default Reports settings that are applied to all Managed Objects, refer to See Configure Reports Settings for more information.

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **audited_system** → **Reports**. Click **Configure** in the **Configure Reports** section, or switch to the **Reports Settings** tab.
2. Specify or modify the following parameters:

Setting	Description
Enable Reports	Select this option to enable the Reports functionality for the selected Managed Object.
	SQL Server Connection
Default	Select this option to use the default SQL Server settings. **NOTE:** The default settings are configured when you create the first Managed Object and enable the Reports functionality in the **New Managed Object** wizard. If you have not specified the default Reports settings before, navigate to **Settings** → **Reports** and click **Modify** to launch the **Reports Configuration** wizard.
Custom	Select this option to specify the custom SQL Server settings that will be applied only to the selected Managed Object and audited system.
SQL Server instance	Specify the name of an existing SQL Server instance where a database for audit data will be created.
Database	Specify the database name.
Windows authentication	Select this option if you want to use the default Data Processing Account to access the SQL database. This account must be granted **database owner (dbo)** 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)** role. Refer to Netwrix Auditor Installation and Configuration Guide for more information.

Setting	Description
Password	Enter a password for the SQL Server authentication.
Report Server URL	Specify the Report Server URL and click **Verify** to ensure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL and click **Verify** to ensure that the resource is reachable.
	Database Retention
Store audit data in the database for x days	Specify the retention period for audit data in days. Old data will be deleted automatically from the SQL database after the specified period. **NOTE:** This option is not available for some of the audited systems. If it is disabled, you can configure the database retention policy by executing a script. See To configure database retention policy for more information.
Clear all database entries	Click **Clear** if you want to delete all audit data from the SQL database.

To upload reports to the Report Server

A report is uploaded to the Report Server the first time you open it in the Netwrix Auditor console. If you want to make reports accessible via a web browser through the SQL Server Report Manager interface, you need to upload reports centrally by doing the following:

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **audited_system** → **Reports**.
2. Click **Upload** in the **Configure Reports** section. You will be notified on successful operation completion.

To assign permissions to view reports

By default, reports are accessible via a web browser through the SQL Server Report Manager interface only by members of the **Domain Admins** group. If you want other users to have access to reports, do the following:

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **audited_system** → **Reports**.
2. Click **Assign** in the **Configure Reports** section.

3. In the dialog that opens, click **Add** and specify the name of the user or group that you want to assign access permissions to. You can search for users or groups inside your Active Directory domain.

To configure database retention policy

If you want audit data to be deleted automatically from your SQL database after a certain period of time, you can specify the retention policy for audit data. For some of the audited systems, you can configure this setting in the Netwrix Auditor console (for details see To specify SQL Server settings). For other audited systems, you need to execute a script. To do this:

1. Navigate to **Start** → **All Programs** → **Microsoft SQL Server** → **SQL Server Management Studio** and connect to your SQL Server instance.
2. In the left pane, navigate to the target database, right-click it and select **New Query** from the pop-up menu.
3. Copy the script below and paste it into the **Query** tab:

```
DECLARE @Retention_Period_Days int SET @Retention_Period_Days = 90 --Please specify the retention
period in days (1 or more).
/*****************************************************************************************/
DECLARE @DB sysname SET @DB = DB_NAME() exec sp_executesql N' USE [msdb]; IF EXISTS (SELECT job_
id FROM msdb.dbo.sysjobs_view WHERE name = N''Retention Job'') BEGIN declare @j_id
uniqueidentifier SELECT @j_id=job_id FROM msdb.dbo.sysjobs_view WHERE name = N''Retention Job''
EXEC msdb.dbo.sp_delete_job @job_id=@j_id, @delete_unused_schedule=1 END; USE [msdb]; BEGIN
TRANSACTION DECLARE @ReturnCode INT SELECT @ReturnCode = 0 IF NOT EXISTS (SELECT name FROM
msdb.dbo.syscategories WHERE name=N''[Uncategorized (Local)]'' AND category_class=1) BEGIN EXEC
@ReturnCode = msdb.dbo.sp_add_category @class=N''JOB'', @type=N''LOCAL'', @name=N''[Uncategorized
(Local)]'' IF (@@ERROR <> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback END DECLARE @jobId BINARY
(16) DECLARE @desc nvarchar(100) SET @desc = N''A scheduled job that deletes all data that is
older than ''+CAST(@Retention As nvarchar(100))+'' day(s).'' EXEC @ReturnCode = msdb.dbo.sp_add_
job @job_name=N''Retention Job'', @enabled=1, @notify_level_eventlog=0, @notify_level_email=0,
@notify_level_netsend=0, @notify_level_page=0, @delete_level=0, @description=@desc, @category_
name=N''[Uncategorized (Local)]'', @owner_login_name=N''sa'', @job_id = @jobId OUTPUT IF (@@ERROR
<> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback DECLARE @sqlcommand nvarchar(max) SET @sqlcommand
= N'' DECLARE @RetDays int DECLARE @Date datetime Set @RetDays = ''+CAST(@Retention As nvarchar
(100))+'' Set @Date = DATEADD(d, -1*@RetDays, GETUTCDATE()) IF EXISTS (select * from [dbo].
[DBVersion] where ProductId = 0 AND DBVersion = 4) BEGIN BEGIN TRAN IF EXISTS (SELECT * FROM
sys.objects WHERE object_id = OBJECT_ID(N''''[dbo].[GPOPropChanges]'''') AND type in
(N''''U'''')) Delete gpc From GPOPropChanges gpc inner join GPOFolderChanges gfc on
gpc.GPOFolderId = gfc.GPOFolderChangeId inner join Changes c on gfc.ChangeId = c.ChangeId inner
join Sessions s on c.ProductId = s.ProductId and c.SessionId = s.SessionId Where s.Date < @Date
If (@@ERROR>0) GOTO QuitWithRollback IF EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N''''[dbo].[GPOFolderChanges]'''') AND type in (N''''U'''')) Delete gfc From
GPOFolderChanges gfc inner join Changes c on gfc.ChangeId = c.ChangeId inner join Sessions s on
c.ProductId = s.ProductId and c.SessionId = s.SessionId Where s.Date < @Date If (@@ERROR>0) GOTO
QuitWithRollback IF EXISTS (SELECT * FROM sys.objects WHERE object_id = OBJECT_ID(N''''[dbo].
[PropChanges]'''') AND type in (N''''U'''')) Delete pc From PropChanges pc inner join Changes c
on pc.ChangeId = c.ChangeId inner join Sessions s on c.ProductId = s.ProductId and c.SessionId =
s.SessionId Where s.Date < @Date If (@@ERROR>0) GOTO QuitWithRollback IF EXISTS (SELECT * FROM
sys.objects WHERE object_id = OBJECT_ID(N''''[dbo].[ObjProps]'''') AND type in (N''''U''''))
Delete op From ObjProps op inner join Changes c on op.ChangeId = c.ChangeId inner join Sessions s
on c.ProductId = s.ProductId and c.SessionId = s.SessionId Where s.Date < @Date If (@@ERROR>0)
GOTO QuitWithRollback IF EXISTS (SELECT * FROM sys.objects WHERE object_id = OBJECT_ID(N''''
[dbo].[Changes]'''') AND type in (N''''U'''')) Delete c From Changes c inner join Sessions s on
```

```
c.ProductId = s.ProductId and c.SessionId = s.SessionId Where s.Date < @Date If (@@ERROR>0) GOTO
QuitWithRollback IF EXISTS (SELECT * FROM sys.objects WHERE object_id = OBJECT_ID(N''''[dbo].
[Sessions]'''') AND type in (N''''U'''')) Delete s From Sessions s Where s.Date < @Date If
(@@ERROR>0) GOTO QuitWithRollback COMMIT TRANSACTION GOTO EndSave QuitWithRollback: IF
(@@TRANCOUNT > 0) ROLLBACK TRANSACTION EndSave: END IF EXISTS (select * from [dbo].[DBVersion]
where ProductId = 0 AND DBVersion >= 5) BEGIN exec sp_Netwrix_DatabaseMaintenance @Date, 0 END ''
 EXEC @ReturnCode = msdb.dbo.sp_add_jobstep @job_id=@jobId, @step_name=N''Retention Step'',
@step_id=1, @cmdexec_success_code=0, @on_success_action=1, @on_success_step_id=0, @on_fail_
action=2, @on_fail_step_id=0, @retry_attempts=0, @retry_interval=0, @os_run_priority=0,
@subsystem=N''TSQL'', @command=@sqlcommand, @database_name=@DBName, @flags=0 IF (@@ERROR <> 0 OR
@ReturnCode <> 0) GOTO QuitWithRollback EXEC @ReturnCode = msdb.dbo.sp_update_job @job_id =
@jobId, @start_step_id = 1 DECLARE @scheduleId uniqueidentifier IF (@@ERROR <> 0 OR @ReturnCode
<> 0) GOTO QuitWithRollback EXEC @ReturnCode = msdb.dbo.sp_add_jobschedule @job_id=@jobId,
@name=N''Retention Schedule'', @enabled=1, @freq_type=4, @freq_interval=1, @freq_subday_type=1,
@freq_subday_interval=0, @freq_relative_interval=0, @freq_recurrence_factor=0, @active_start_
date=NULL, @active_end_date=99991231, @active_start_time=20000, @active_end_time=235959 IF
(@@ERROR <> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback EXEC @ReturnCode = msdb.dbo.sp_add_
jobserver @job_id = @jobId, @server_name = N''(local)'' IF (@@ERROR <> 0 OR @ReturnCode <> 0)
GOTO QuitWithRollback COMMIT TRANSACTION GOTO EndSave QuitWithRollback: IF (@@TRANCOUNT > 0)
ROLLBACK TRANSACTION EndSave: ', N'@DBName sysname, @Retention int', @DBName = @DB, @Retention =
@Retention_Period_Days
```

4. In the second line of the query, specify the retention period for your audit data in days:

   ```
   SET @Retention_Period_Days = 90
   ```

5. Click **Execute** in the Microsoft SQL Server Management Studio toolbar to execute the query.

To import audit data to a SQL database

If you did not enable the Reports functionality on Managed Object creation and decide to enable it later, you can make audit data stored locally in the Audit Archive available for SSRS-based Reports by importing it with the DB Importer tool. This tool can also be used for data recovery in case the database is corrupted.

This functionality is currently available for the following Netwrix Auditor features:

- Active Directory Auditing
- Event Log Management
- Exchange Server Auditing
- Windows File Server Auditing
- Group Policy Auditing
- SQL Server Auditing
- User Activity Video Recording
- VMware Auditing
- Windows Server Auditing

To import audit data, do the following:

1. Navigate to a Netwrix Auditor feature installation folder, locate **DB Importer**, and double-click to launch it.

2. Select the Managed Object and the time range for which you want to import data and click **Import**.

4.2. Subscriptions

In Netwrix Auditor, you can configure a report subscription to schedule automatic report generation and delivery. You can apply various filters to reports delivered by subscription, and choose their output format (Word, Excel, PDF, etc.). Reports are delivered as email attachments in the selected format.

The subscription functionality is currently supported by the following Netwrix Auditor features:

- Active Directory Auditing
- Event Log Management
- Exchange Server Auditing
- Group Policy Auditing
- SharePoint Auditing
- User Activity Video Recording
- Windows Server Auditing

You can also configure subscriptions for enterprise-wide reports and dashboards.

Refer to the following procedures for detailed instructions:

- To create a subscription
- To force on-demand report delivery

To create a subscription

1. In the Netwrix Auditor console, navigate to the report that you want to subscribe to and click **Subscribe**. Alternatively, navigate to the **Subscriptions** node under **Managed Object** → **your_Managed_Object** → **audited_system** and click **Add**.
2. On the welcome page of the **Report Subscription** wizard, click **Next** and wait until connection to the Report Server is established.
3. On the **Select Report** step, enter the subscription name and description (optional), and specify the report that you want to subscribe to from the drop-down list. If you start the Report Subscription wizard from a specific report page, this field will be filled in automatically.
4. On the **Specify Report Recipients** step, click **Add** and enter the email address where this report will be delivered. Click **Verify** to check your email settings. The product will send a test message to the specified address and will inform you if any problems are detected. You can specify as many recipients as needed.
5. On the **Specify Report Delivery Options and Filters** step, select the report delivery format and select the **Do not send empty reports** option if you do not want reports to be generated if no

changes occurred during the reporting period. Specify the report filters, which vary depending on the selected report.

6. On the **Configure Report Delivery Schedule** step, specify when you want the report to be generated and delivered.
7. On the last step, review your subscription settings and click **Finish**. The new subscription will appear under the **Subscriptions** node for the selected audited system.

If later you need to change the report delivery format or filters, modify the delivery schedule and add or remove report recipients, you can edit your subsription settings on the subscription page.

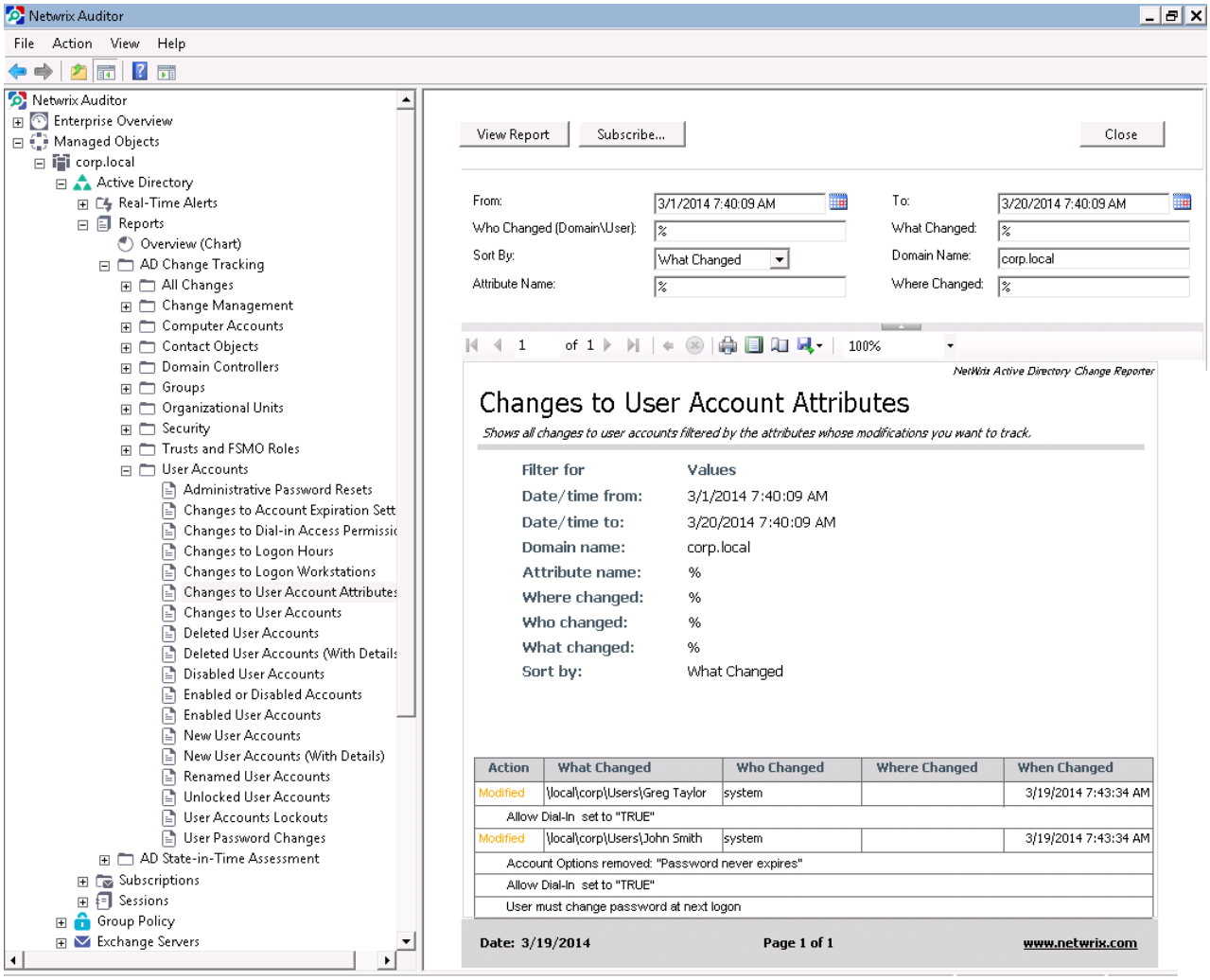
To force on-demand report delivery

You can force an on-demand delivery of any report that you have configured a subscription for. To do this:

1. In the Netwrix Auditor console, navigate to the to the **Subscriptions** node under **your_Managed_Object** → **audited_system** and the select the subscription for the report that you want to generate and send now.
2. On the report subscription page, click **Generate Now**. The report will be generated and delivered to the specified recipients. It will contain audit data starting from the last scheduled report delivery (or from subscription creation time if no scheduled deliveries have been performed so far) and until the last scheduled data collection time (3:00 AM by default).

4.3. Change Reports

Change reports can be found under the **Reports** node for the selected audited system. They are grouped into folders and provide the information on changes to different aspects of the audited environment. Each change report has a set of filters which help organize audit data in the most convenient way.



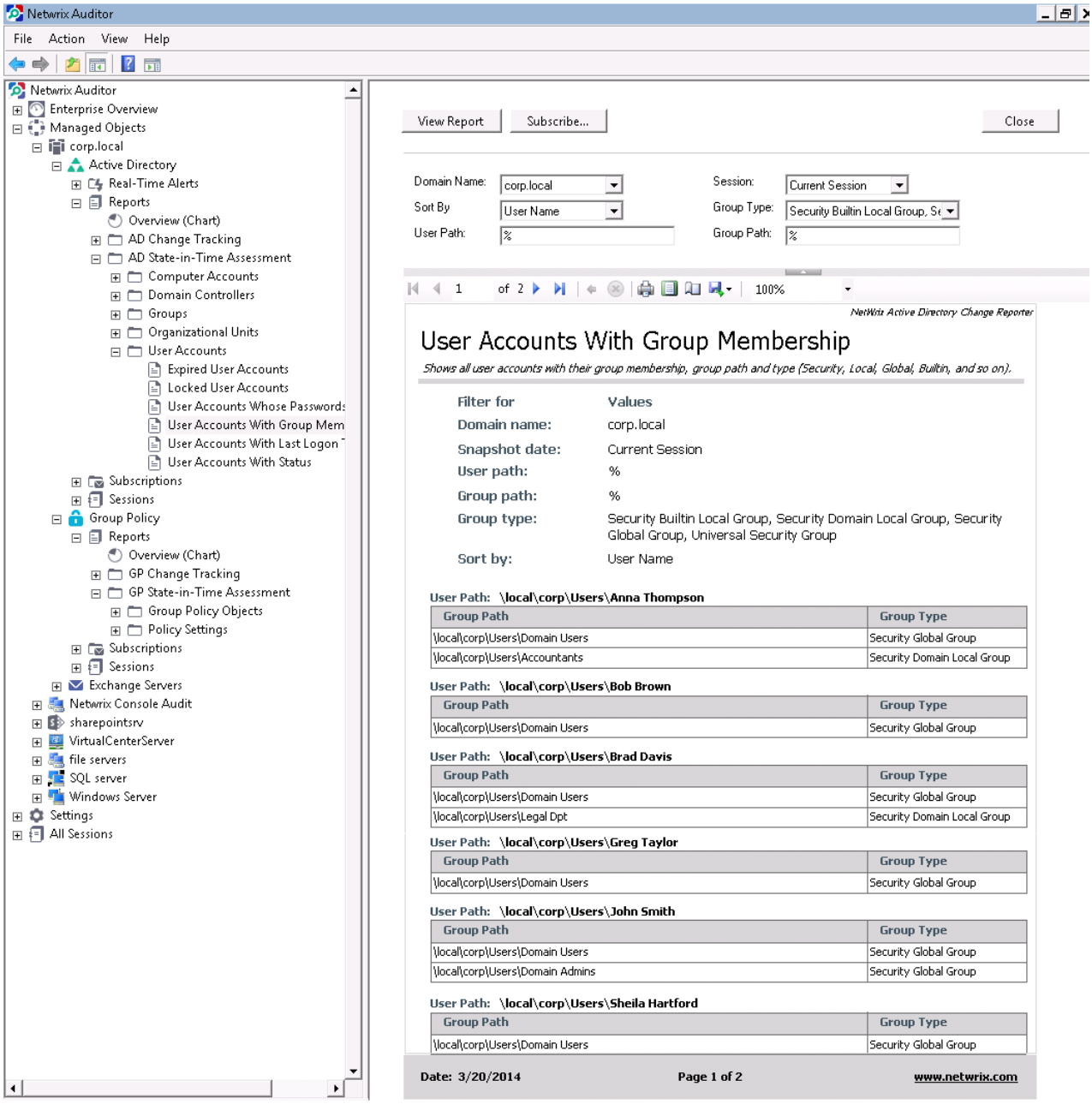
4.4. State-in-Time Reports

The state -in-time reports functionality allows generating reports on the configuration state of the audited system at a specific moment of time in addition to change reports. State-in-time reports are based on the configuration snapshots captured by the product daily, and reflect a particular aspect of the audited environment.

This functionality is currently available for the following Netwrix Auditor features:

- Active Directory Auditing
- Group Policy Auditing

The state-in-time reports are found in the State-in-Time Assessment folder under the **Reports** node for the selected audited system. Each state-in-time report has a set of filters which help organize audit data in the most convenient way.



By default, state-in-time reports reflect the current configuration state of the audited system. If you want to generate a report to assess your system at a particular moment in the past, you can select the corresponding snapshot from the **Session** filter.

To be able to generate reports based on different snapshots, you need to import them to the SQL database, otherwise only the **Current Session** option is available.

To import historical snapshots to the SQL database

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **audited_system** → **Reports** and switch to the **State-in-Time Reports** tab.

2. In the **Historical Snapshot Management** sestion, select the snapshots that you want to import to the SQL database, and move them to the **Snapshots available for reporting** list using the arrow button.
3. Click **Apply** to save the changes and wait until connection to the Report Server is established and snapshots are imported.

NOTE: You need to close any open state-in-time reports before the imported snaphosts become available in the **Session** filter.

4.5. Overview Reports

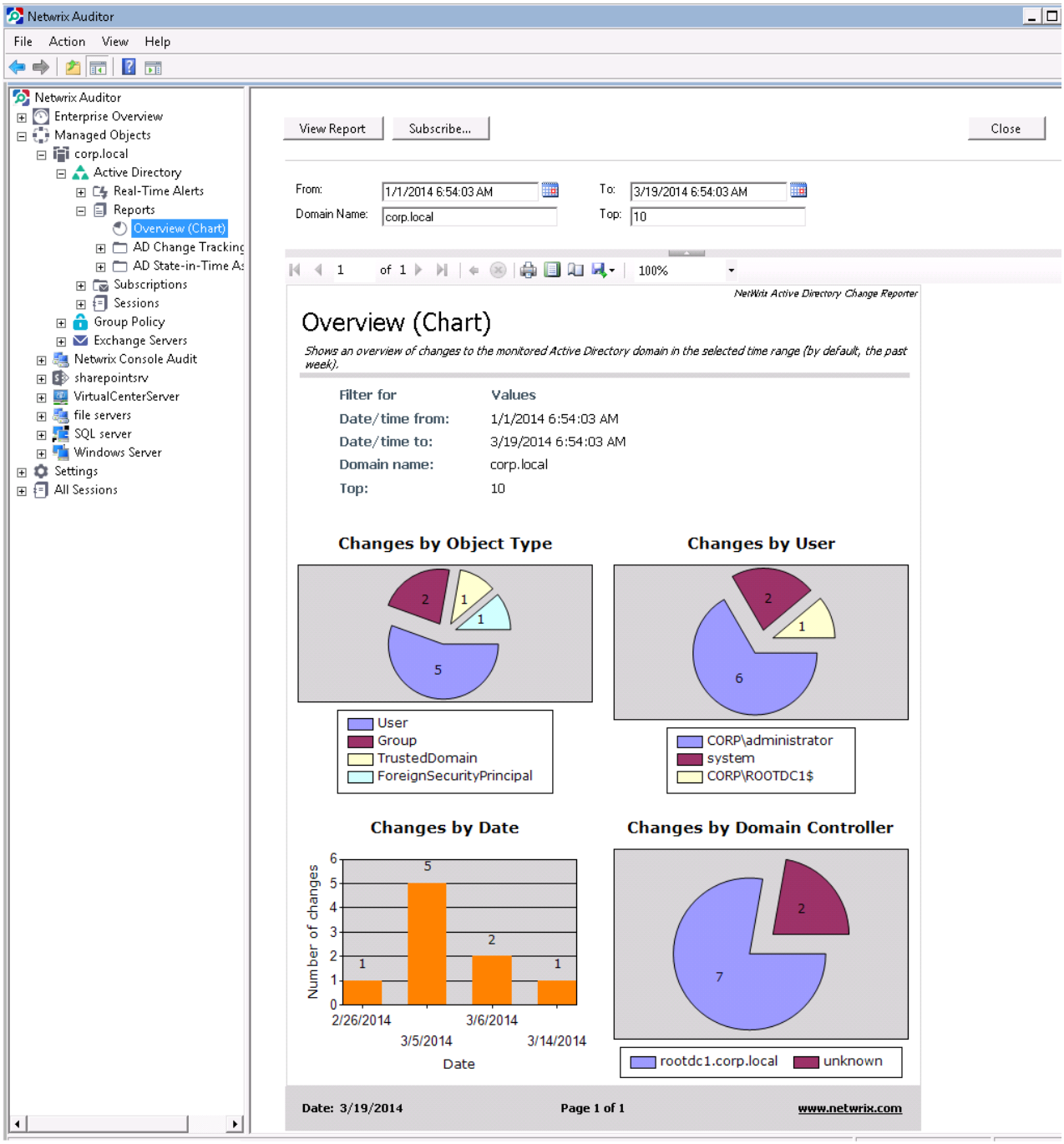
Overview reports are chart reports that provide a high-level overview of changes to the audited environment within the selected time period. Overview reports consist of four charts, showing the activity trends by date, user, object type and server (or domain controller).

Chart reports provide the drill-through functionality, which means that by clicking on a chart segment, you will be redirected to a table report with the corresponding filtering and grouping of data that renders the next level of detail.

This functionality is currently available for the following Netwrix Auditor features:

- Active Directory Auditing
- Exchange Server Auditing
- Group Policy Auditing
- Windows Server Auditing
- SharePoint Auditing
- User Activity Video Recording

Overview reports can be found under the **Reports** node for the selected audited system.



4.6. Change Review History Reports

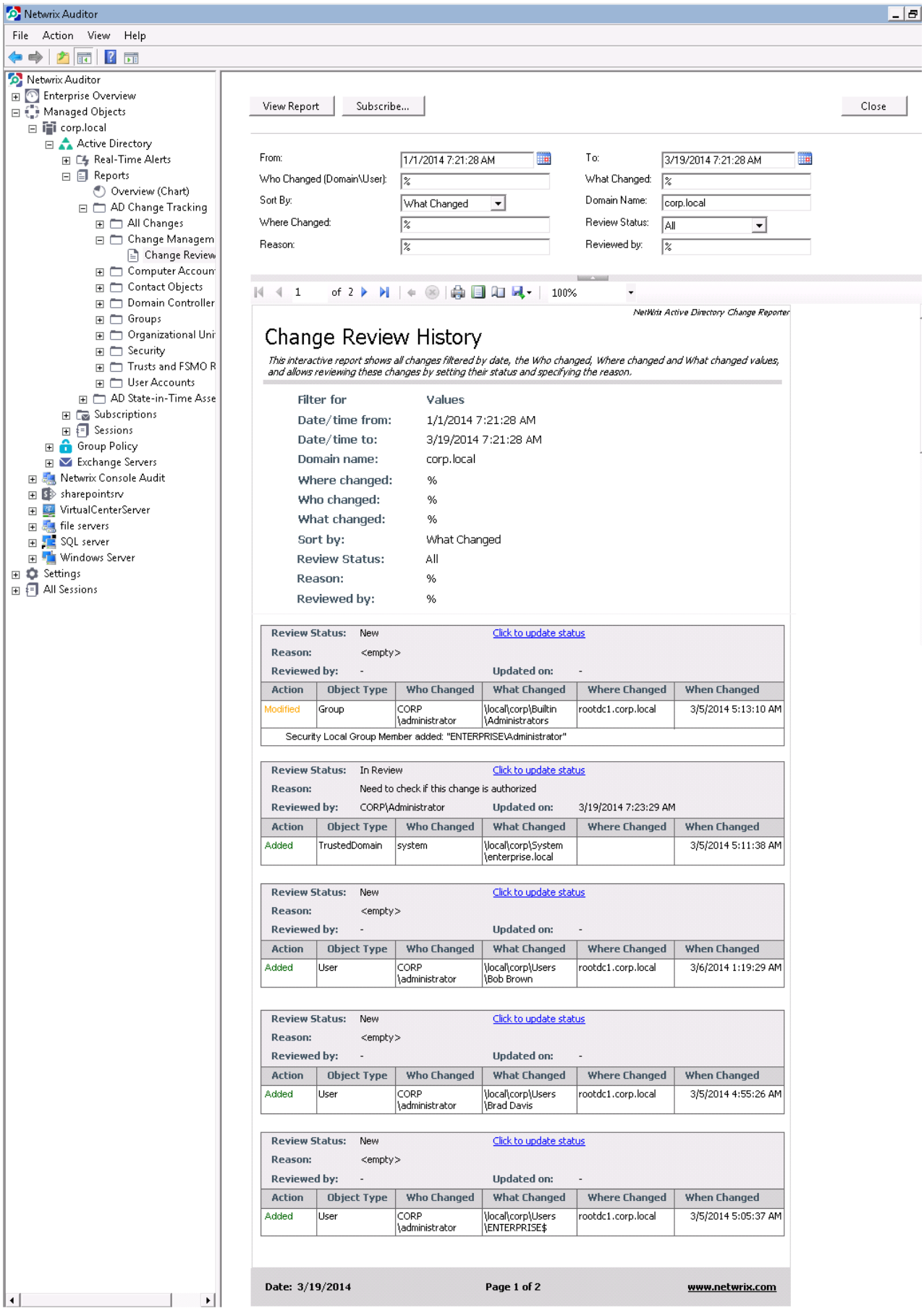
Change management is one of the critical processes for many companies referring to such areas as requesting, planning, implementing, and evaluating changes to various systems. Netwrix Auditor allows facilitating the change auditing process by providing the change monitoring and reporting capabilities. Additionally, you can review and assign such properties as a review status and reason for each change made to the audited systems.

This functionality is currently available for the following Netwrix Auditor features:

- Active Directory Auditing
- Exchange Server Auditing
- Group Policy Auditing
- SharePoint Auditing
- Windows Server Auditing

Change Review History reports are found in the **Change Management** folder under the **Reports** node for the selected audited system. They list all changes to the monitored environment that are assigned the **New** status by default. If a change seems unauthorized, or requires further analysis, you can click the **Click to update status** link, set its status to **In Review** and provide a reason. Once the change has been approved of, or rolled back, you can set its status to **Resolved**.

NOTE: If you are updating the status of a change in a web browser, and the text in the comment field contains more than 150 characters, you will not be able to change the status for this change once again.


Netwrix Auditor
File Action View Help
Netwrix Auditor
Enterprise Overview
Managed Objects
corp.local
Active Directory
Real-Time Alerts
Reports
Overview (Chart)
AD Change Tracking
All Changes
Change Managem
Change Review
Computer Accoun
Contact Objects
Domain Controller
Groups
Organizational Uni
Security
Trusts and FSMO R
User Accounts
AD State-in-Time Asse
Subscriptions
Sessions
Group Policy
Exchange Servers
Netwrix Console Audit
sharepointsrv
VirtualCenterServer
file servers
SQL server
Windows Server
Settings
All Sessions
View Report
Subscribe...
Close
From: 1/1/2014 7:21:28 AM
To: 3/19/2014 7:21:28 AM
Who Changed (Domain\User): %
What Changed: %
Sort By: What Changed
Domain Name: corp.local
Where Changed: %
Review Status: All
Reason: %
Reviewed by: %
1 of 2
100%
NetWrix Active Directory Change Reporter
Change Review History
This interactive report shows all changes filtered by date, the Who changed, Where changed and What changed values, and allows reviewing these changes by setting their status and specifying the reason.
Filter for Values
Date/time from: 1/1/2014 7:21:28 AM
Date/time to: 3/19/2014 7:21:28 AM
Domain name: corp.local
Where changed: %
Who changed: %
What changed: %
Sort by: What Changed
Review Status: All
Reason: %
Reviewed by: %
Review Status: New Click to update status
Reason: <empty>
Reviewed by: - Updated on: -
Action Object Type Who Changed What Changed Where Changed When Changed
Modified Group CORP \administrator \local\corp\Builtin \Administrators rootdc1.corp.local 3/5/2014 5:13:10 AM
Security Local Group Member added: "ENTERPRISE\Administrator"
Review Status: In Review Click to update status
Reason: Need to check if this change is authorized
Reviewed by: CORP\Administrator Updated on: 3/19/2014 7:23:29 AM
Action Object Type Who Changed What Changed Where Changed When Changed
Added TrustedDomain system \local\corp\System \enterprise.local 3/5/2014 5:11:38 AM
Review Status: New Click to update status
Reason: <empty>
Reviewed by: - Updated on: -
Action Object Type Who Changed What Changed Where Changed When Changed
Added User CORP \administrator \local\corp\Users \Bob Brown rootdc1.corp.local 3/6/2014 1:19:29 AM
Review Status: New Click to update status
Reason: <empty>
Reviewed by: - Updated on: -
Action Object Type Who Changed What Changed Where Changed When Changed
Added User CORP \administrator \local\corp\Users \Brad Davis rootdc1.corp.local 3/5/2014 4:55:26 AM
Review Status: New Click to update status
Reason: <empty>
Reviewed by: - Updated on: -
Action Object Type Who Changed What Changed Where Changed When Changed
Added User CORP \administrator \local\corp\Users \ENTERPRISE$ rootdc1.corp.local 3/5/2014 5:05:37 AM
Date: 3/19/2014 Page 1 of 2 www.netwrix.com

4.7. Reports with Extended Audit Data

By default, Netwrix Auditor is configured to collect the following additional audit data:

- Originating workstation: the name of the computer where the user was logged on when they made the change. See Reports with Originating Workstation for more information.
- Group membership: the list of Active Directory groups that the user who made the change belonged to at the time when the change was made. See Reports with Data Filtering by Groups for more information.

This functionality is currently available for the following Netwrix Auditor features:

- Active Directory Auditing
- Exchange Server Auditing
- Group Policy Auditing
- SharePoint Auditing

NOTE: If the product is configured to collect data on the originating workstation, additional events are written to the Security event log, which may lead to data overwrites. To prevent data loss, it is recommended to configure the maximum size and retention settings of the Security log (for detailed instructions, refer to Netwrix Auditor Installation and Configuration Guide).

For the product to be able to collect the information on the originating workstation, you must configure the **Audit logon events** policy. If automatic audit configuration is enabled, this setting is adjusted automatically. For instructions on how to configure it manually, refer to Netwrix Auditor Installation and Configuration Guide.

To disable collection of additional audit data

If you do not want the product to collect additional audit data, follow the instructions in the table below depending on the Netwrix Auditor feature:

Feature	Instructions
Active Directory Auditing Exchange Server Auditing Group Policy Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Active Directory** / **Exchange Server** / **Group Policy**. 2. In the right pane, click **Configure** next to **Advanced Options**. 3. In the dialog that opens, deselect the **Originating workstation** and the **Group membership** option. **NOTE:** If you disable these options for one of these Netwrix Auditor features, it will also be disabled for the other two.

Feature	Instructions
SharePoint Auditing	1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **SharePoint**. 2. In the right pane, click **Configure Options** next to **Options**. 3. In the dialog that opens, deselect the **Originating workstation** and the **Group membership** option.

4.7.1. Reports with Originating Workstation

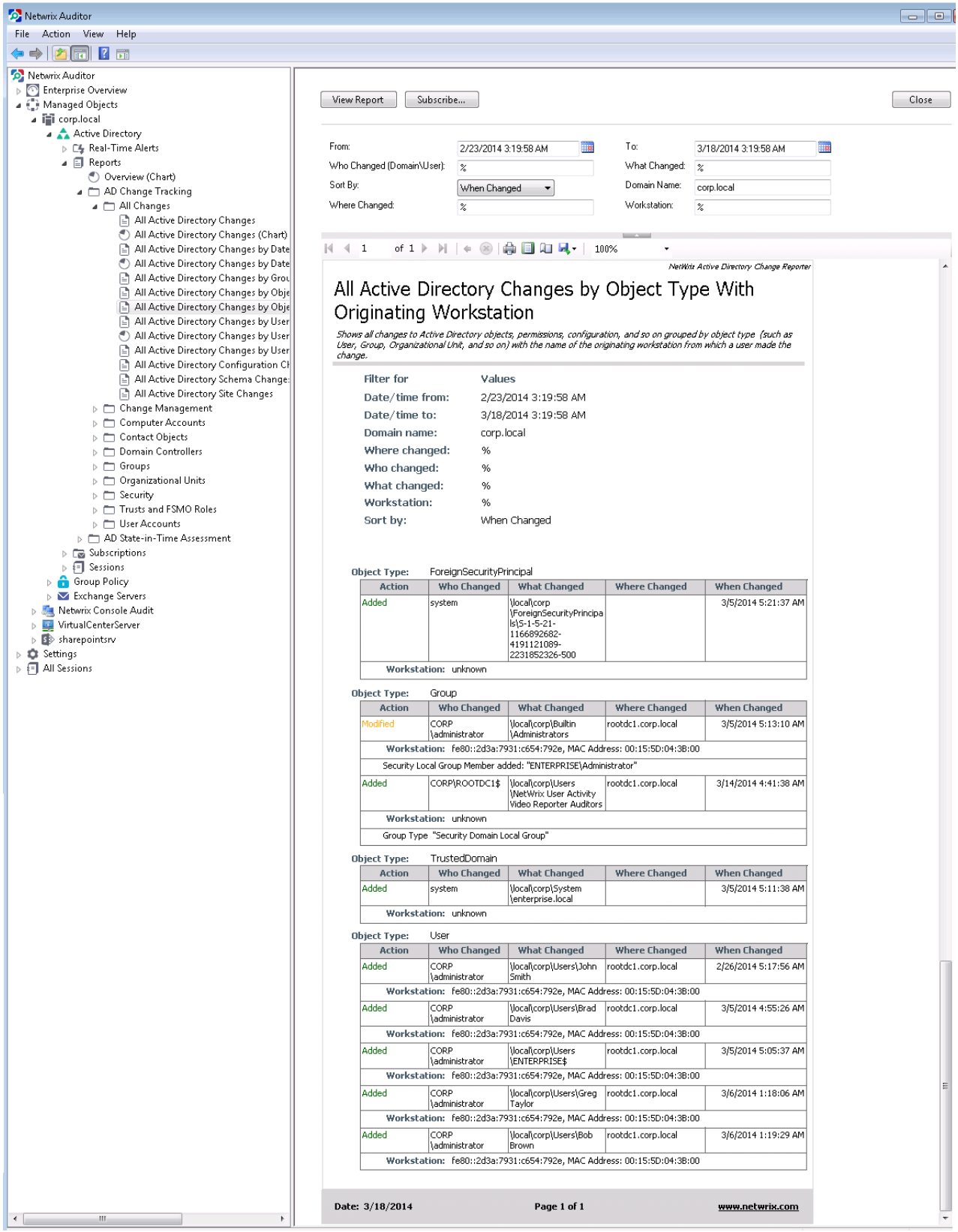
Netwrix Auditor provides a number of reports that, in addition to the standard *who*, *when*, *where* and *when* fields, provide the information on the originating workstation, i.e. the name of the computer where the user was logged on when they made the change.

The following reports with the additional field are available:

Feature	Report Name	Report Path
Active Directory Auditing	All Active Directory Changes by Groups With Originating Workstation	Managed Objects → your_Managed_Object → Active Directory → Reports → AD Change Tracking → All Changes
	All Active Directory Changes by Object Type With Originating Workstation	
	All Active Directory Changes by User With Originating Workstation	
Exchange Server Auditing	All MS Exchange Changes by Groups With Originating Workstation	Managed Objects → your_Managed_Object → Exchange Server → Reports → All Changes
	All MS Exchange Changes by Object Type With Originating Workstation	
	All MS Exchange Changes by Server With Originating Workstation	
	All MS Exchange Changes by User With Originating Workstation	
Group Policy Auditing	All Group Policy Changes by Groups With Originating Workstation	Managed Objects → your_Managed_Object → Group Policy → Reports → GP Change Tracking → All Changes
	All Group Policy Changes With Originating Workstation	

Feature	Report Name	Report Path
SharePoint Auditing	All SharePoint Changes	Managed Objects → your_Managed_Object → SharePoint → Reports → All Changes
	All SharePoint Content Changes by User	
	Change Review History	Managed Objects → your_Managed_Object → SharePoint → Reports → Change Management

In these reports, the Workstation field under each change provides the name/IP address of the computer from which the change was made:


Netwrix Auditor
File Action View Help
Netwrix Auditor
Enterprise Overview
Managed Objects
corp.local
Active Directory
Real-Time Alerts
Reports
Overview (Chart)
AD Change Tracking
All Changes
All Active Directory Changes
All Active Directory Changes (Chart)
All Active Directory Changes by Date
All Active Directory Changes by Date
All Active Directory Changes by Grou
All Active Directory Changes by Obje
All Active Directory Changes by Obje
All Active Directory Changes by User
All Active Directory Changes by User
All Active Directory Changes by User
All Active Directory Configuration Ch
All Active Directory Schema Change:
All Active Directory Site Changes
Change Management
Computer Accounts
Contact Objects
Domain Controllers
Groups
Organizational Units
Security
Trusts and FSMO Roles
User Accounts
AD State-in-Time Assessment
Subscriptions
Sessions
Group Policy
Exchange Servers
Netwrix Console Audit
VirtualCenterServer
sharepointsrv
Settings
All Sessions
View Report
Subscribe...
Close
From: 2/23/2014 3:19:58 AM
To: 3/18/2014 3:19:58 AM
Who Changed (Domain\User): %
What Changed: %
Sort By: When Changed
Domain Name: corp.local
Where Changed: %
Workstation: %
1 of 1
100%
NetWrix Active Directory Change Reporter
All Active Directory Changes by Object Type With Originating Workstation
Shows all changes to Active Directory objects, permissions, configuration, and so on grouped by object type (such as User, Group, Organizational Unit, and so on) with the name of the originating workstation from which a user made the change.
Filter for Values
Date/time from: 2/23/2014 3:19:58 AM
Date/time to: 3/18/2014 3:19:58 AM
Domain name: corp.local
Where changed: %
Who changed: %
What changed: %
Workstation: %
Sort by: When Changed
Object Type: ForeignSecurityPrincipal
Action Who Changed What Changed Where Changed When Changed
Added system \local\corp\ForeignSecurityPrincipals\S-1-5-21-1166892682-4191121089-2231852326-500 3/5/2014 5:21:37 AM
Workstation: unknown
Object Type: Group
Action Who Changed What Changed Where Changed When Changed
Modified CORP\administrator \local\corp\Builtin\Administrators rootdc1.corp.local 3/5/2014 5:13:10 AM
Workstation: fe80::2d3a:7931:c654:792e, MAC Address: 00:15:5D:04:3B:00
Security Local Group Member added: "ENTERPRISE\Administrator"
Added CORP\ROOTDC1$ \local\corp\Users\NetWrix User Activity Video Reporter Auditors rootdc1.corp.local 3/14/2014 4:41:38 AM
Workstation: unknown
Group Type "Security Domain Local Group"
Object Type: TrustedDomain
Action Who Changed What Changed Where Changed When Changed
Added system \local\corp\System\enterprise.local 3/5/2014 5:11:38 AM
Workstation: unknown
Object Type: User
Action Who Changed What Changed Where Changed When Changed
Added CORP\administrator \local\corp\Users\John Smith rootdc1.corp.local 2/26/2014 5:17:56 AM
Workstation: fe80::2d3a:7931:c654:792e, MAC Address: 00:15:5D:04:3B:00
Added CORP\administrator \local\corp\Users\Brad Davis rootdc1.corp.local 3/5/2014 4:55:26 AM
Workstation: fe80::2d3a:7931:c654:792e, MAC Address: 00:15:5D:04:3B:00
Added CORP\administrator \local\corp\Users\ENTERPRISE$ rootdc1.corp.local 3/5/2014 5:05:37 AM
Workstation: fe80::2d3a:7931:c654:792e, MAC Address: 00:15:5D:04:3B:00
Added CORP\administrator \local\corp\Users\Greg Taylor rootdc1.corp.local 3/6/2014 1:18:06 AM
Workstation: fe80::2d3a:7931:c654:792e, MAC Address: 00:15:5D:04:3B:00
Added CORP\administrator \local\corp\Users\Bob Brown rootdc1.corp.local 3/6/2014 1:19:29 AM
Workstation: fe80::2d3a:7931:c654:792e, MAC Address: 00:15:5D:04:3B:00
Date: 3/18/2014 Page 1 of 1 www.netwrix.com

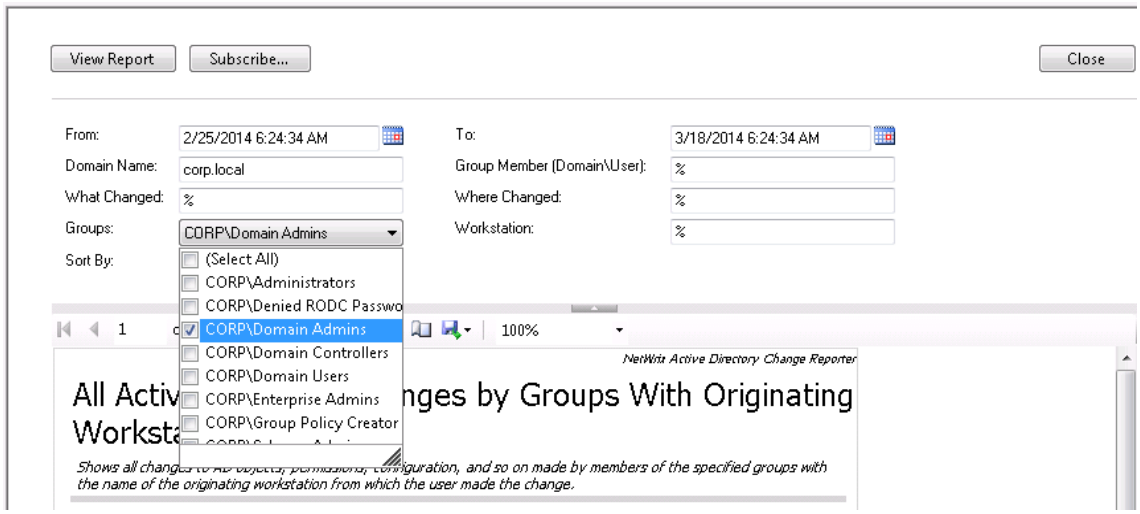
4.7.2. Reports with Data Filtering by Groups

The information on AD group membership of the users who make the changes can be used to apply filters to the collected audit data and get the information on changes performed by members of specific groups only.

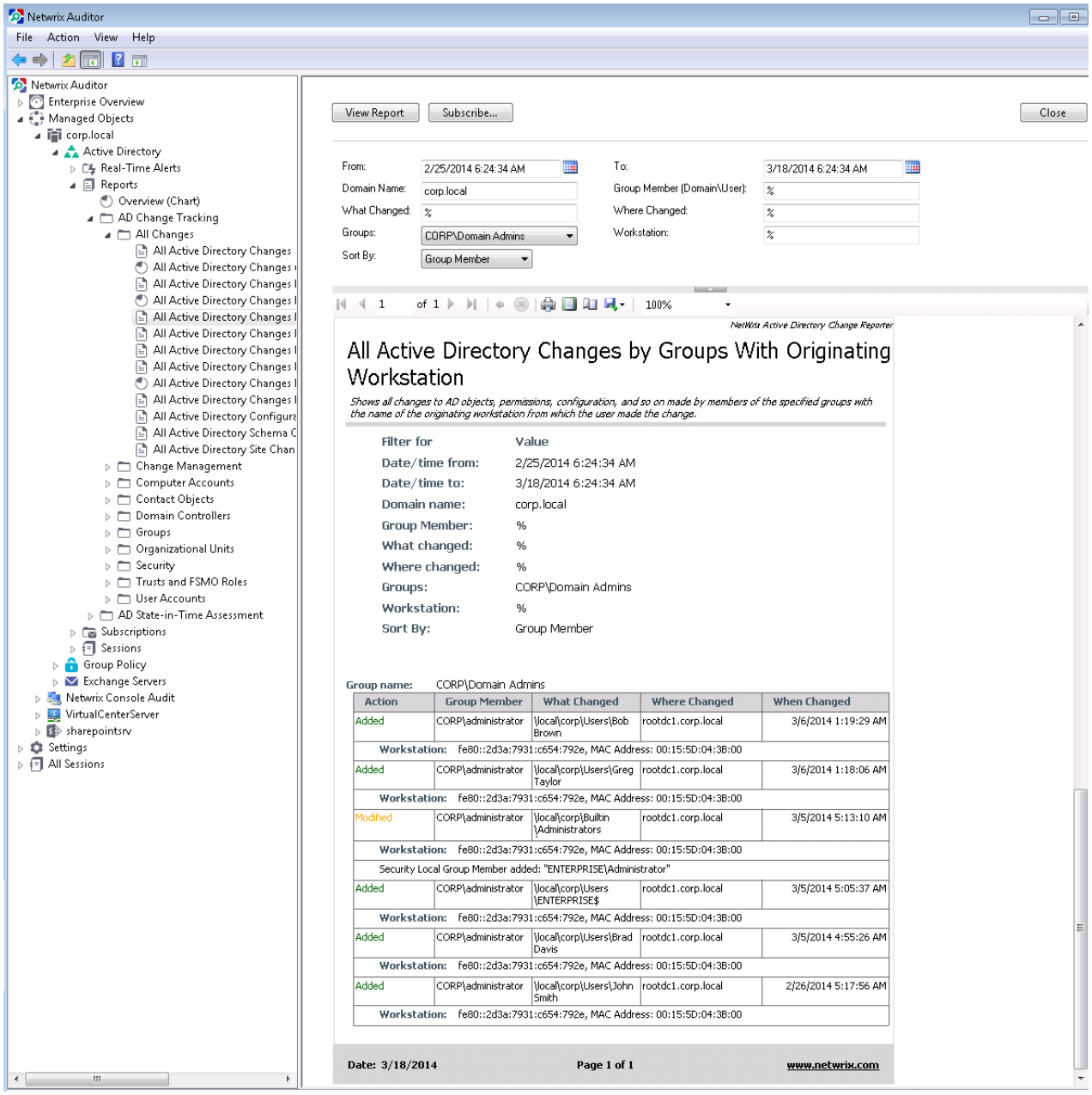
The following reports with data filtering by group membership are available:

Feature	Report Name	Report Path
Active Directory Auditing	All Active Directory Changes by Groups With Originating Workstation	Managed Objects → your_Managed_ Object → Active Directory → Reports → AD Change Tracking → All Changes
Exchange Server Auditing	All MS Exchange Changes by Groups With Originating Workstation	Managed Objects → your_Managed_ Object → Exchange Servers → Reports → All Changes
Group Policy Auditing	All Group Policy Changes by Groups With Originating Workstation	Managed Objects → your_Managed_ Object → Group Policy → Reports → GP Change Tracking → All Changes
SharePoint Auditing	All SharePoint Changes	Managed Objects → your_Managed_ Object → SharePoint → Reports → All Changes
	All SharePoint Content Changes by User	
	All SharePoint Permission Changes by User	
	Change Review History	Managed Objects → your_Managed_ Object → SharePoint → Reports → Change Management

If you want to get the information on changes performed by members of a specific group, select this group (or several groups) in the corresponding filter, and click View Report:

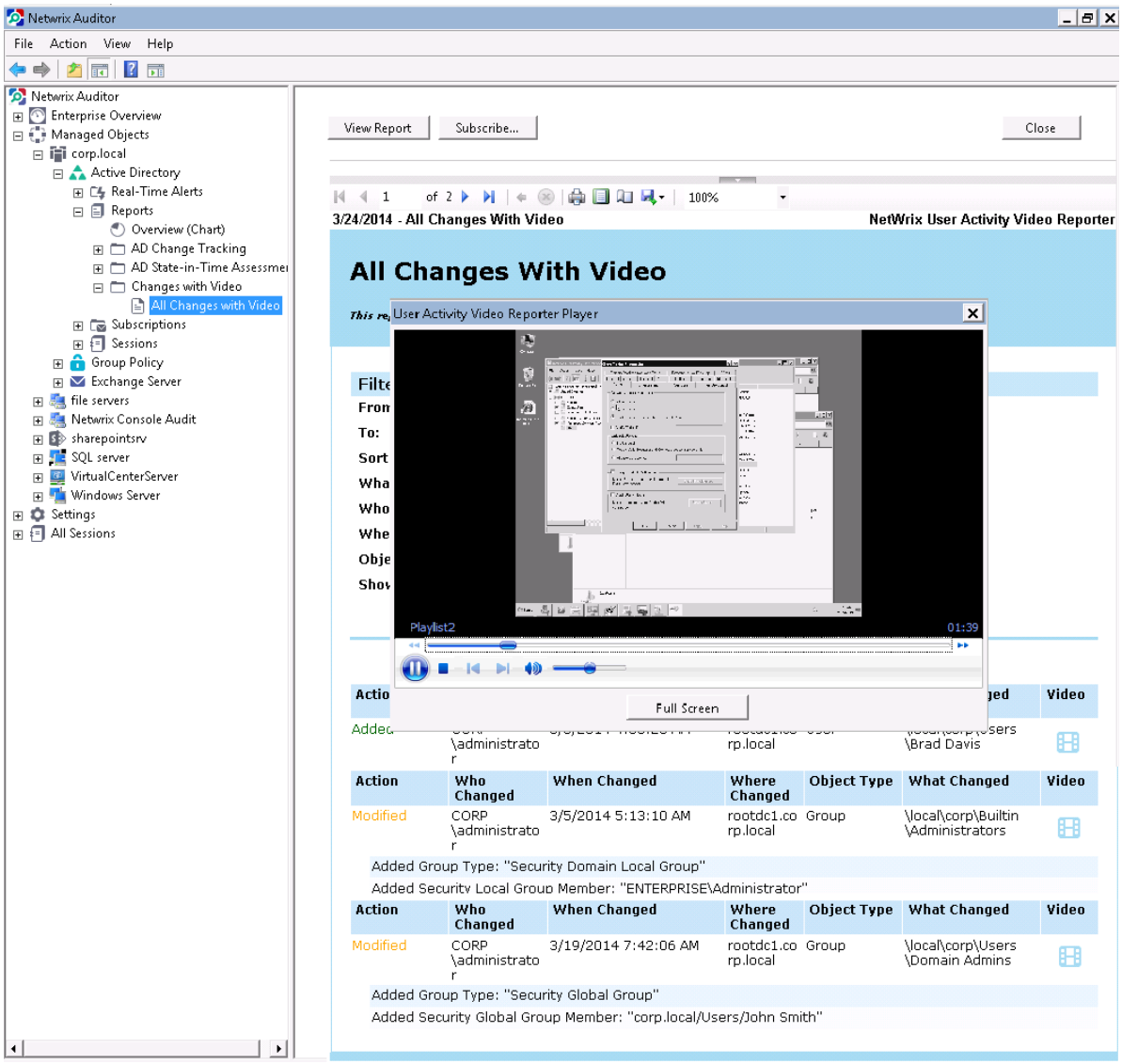


The report will only show the changes made by members of the selected group(s):



4.8. Reports with Video

The User Activity Video Recording feature of Netwrix Auditor tracks users activity on the audited computers and saves video records. By integrating it with the other product features, you can get reports with links to video records. When you click a link, a video player will open and playback of the recorded user session will start, showing you *how* each particular change was made:



This functionality is currently available for the following Netwrix Auditor features:

- Active Directory Auditing
- Exchange Server Auditing
- Group Policy Auditing
- SharePoint Auditing
- SQL Server Auditing
- Windows File Server Auditing
- Windows Server Auditing

To integrate video records into change reports

Integration of the User Activity Video Recording feature with the other Netwrix Auditor features can be performed if the following conditions are met:

- The Reports functionality is enabled and configured for both the User Activity Video Recording feature and the feature you want to integrate with.
- The audit database of the User Activity Video Recording feature resides on the same SQL Server instance as the audit database for the Netwrix Auditor feature you want to integrate with.

1. Configure the User Activity Video Recording feature for the Managed Object that contains the audited system you want to integrate with.

   NOTE: If you want to integrate video records into change reports of a Netwrix Auditor feature that uses a different Managed Object type (other than Computer Collection), it is recommended to create a dedicated Managed Object with the User Activity Video Recording feature enabled that contains the workstations / servers / domain controllers audited within the scope of the original Managed Object.

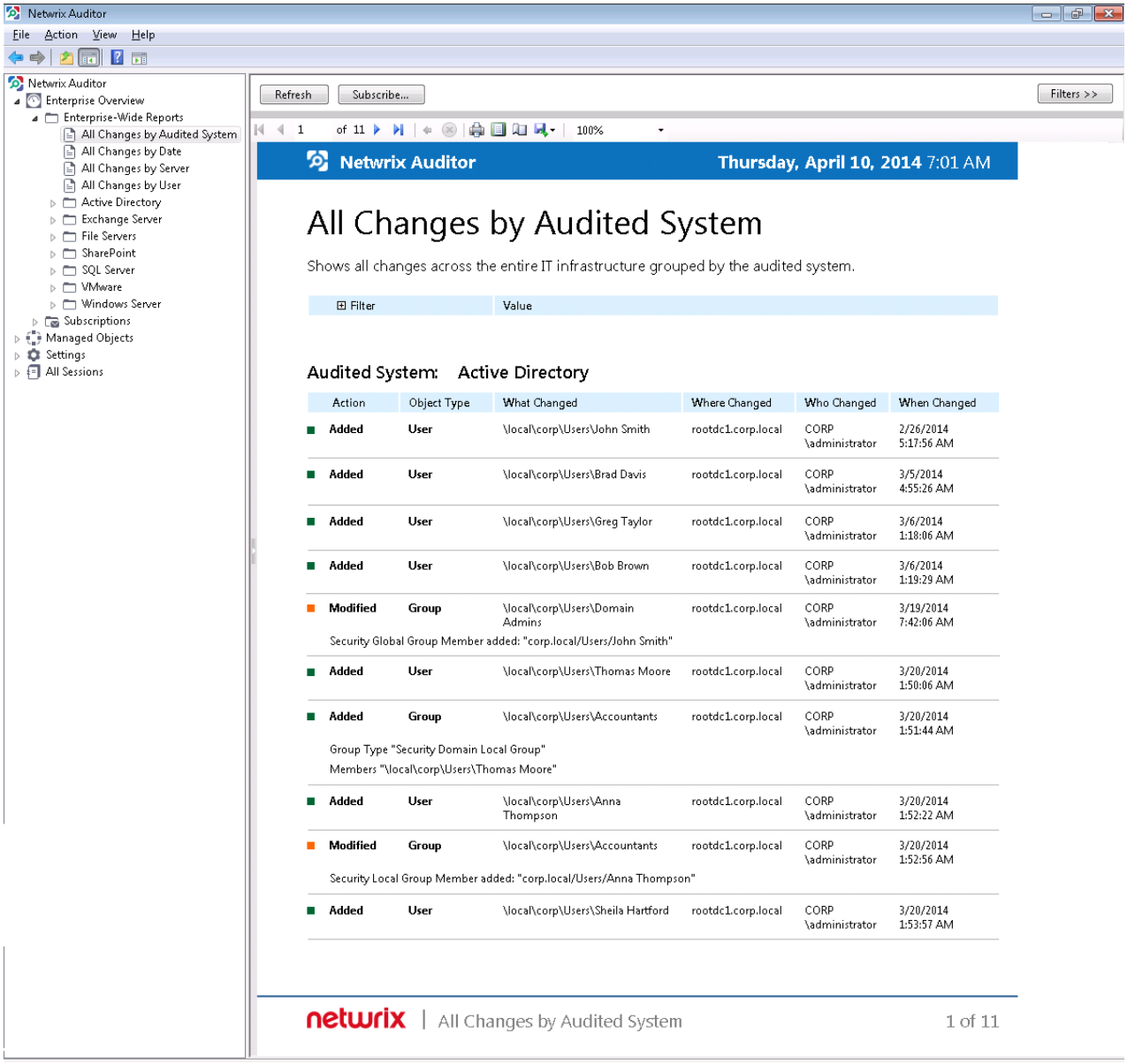
2. Under this Managed Object, navigate to the **User Activity** node and click the **Integrate video records** link in the right pane.
3. In the dialog that opens, select the audited system and the Managed Object that you want to integrate with and click **Integrate**. When the operation has completed successfully, the status of the selected audited system will change to "Integrated".
4. Restart the Netwrix Auditor console for the changes to take effect.

   Once you have configured integration with the User Activity Video Recording feature, the **Changes with Video** subfolder containing the **All Changes with video** report will be added to the **Reports** folder under the selected audited system.

4.9. Enterprise-Wide Reports

Enterprise-Wide reports aggregate data from all Managed Objects. Common reports list changes that occurred across all audited systems, while system-specific reports aggregate data from all Managed Objects where audit of this system is enabled.

Enterprise-Wide reports can be found under the **Enterprise Overview** → **Enterprise-Wide Reports** node.



4.10. Dashboards

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.

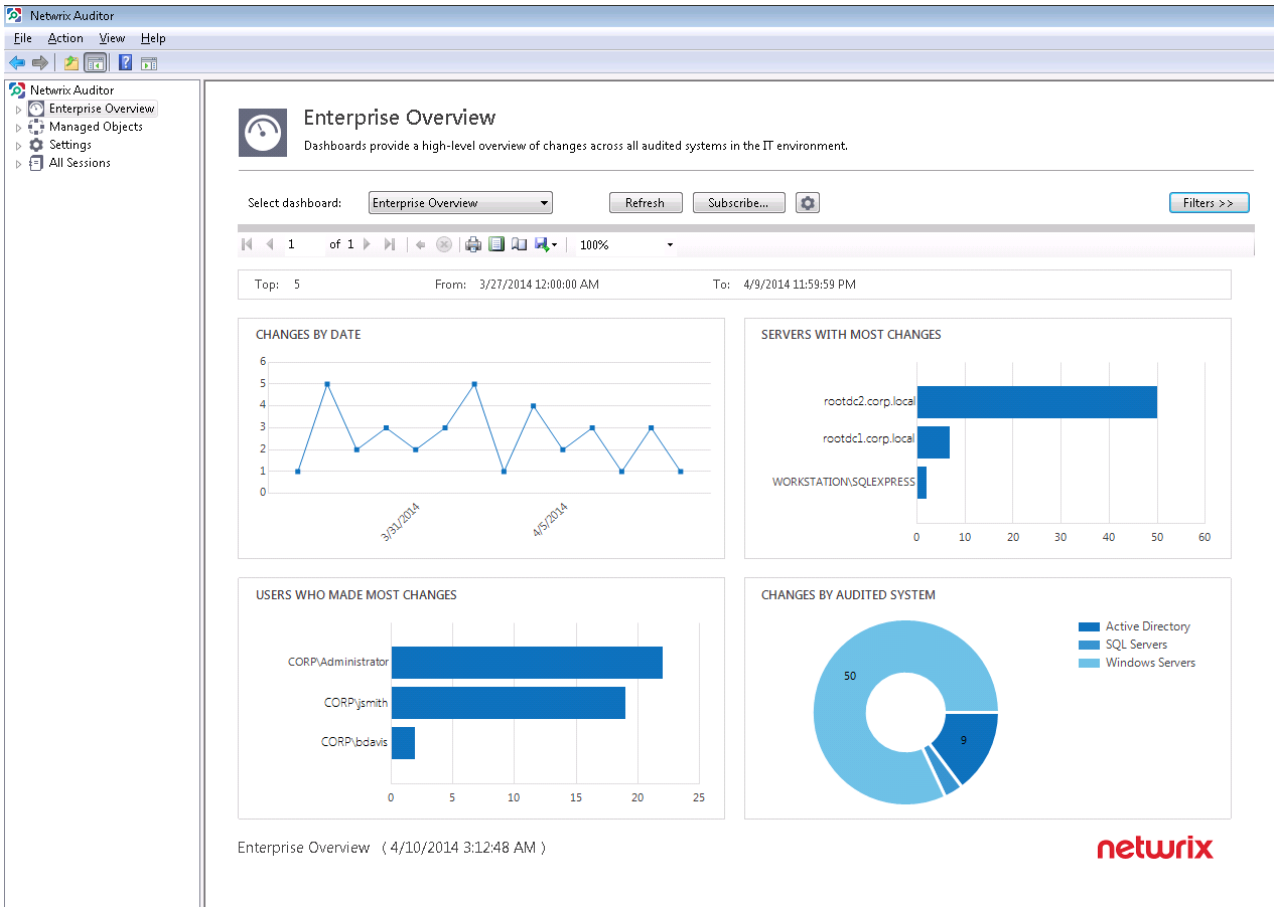
The current version of Netwrix Auditor contains the following dashboards:

- Enterprise Overview (aggregates data on all audited systems listed below)
- Active Directory Overview
- Exchange Server Overview
- File Servers Overview

- SharePoint Overview
- SQL Server Overview
- VMware Overview
- Windows Server Overview

All dashboards provide the drill-through functionality, which means that by clicking on a chart segment, you will be redirected to a table report with the corresponding filtering and grouping of data that renders the next level of detail. See Enterprise-Wide Reports for more information.

Dashboards are available on the Enterprise Overview node:



NOTE: In a production environment, data collection occurs daily (it is scheduled to 3:00 AM by default). The default filters in dashboards are set to show data for the last 14 days. The current date is not included in the reporting scope to avoid displaying incomplete audit data.

5. Configure Real-Time Alerts

If you want to be notified immediately about changes to certain objects, you can configure Real-Time Alerts that will be triggered by specific events. Alerts are emailed immediately after the specified event has been detected.

This functionality is currently available for the following Netwrix Auditor features:

- Active Directory Auditing
- Event Log Management (including alerts for Mailbox Access Auditing)

You can create your own custom alerts and enable / disable and modify the predefined Real-Time Alerts provided by Netwrix. To do it, perform the following procedures:

To..	In the Netwrix Auditor console	In the Managed Object wizard
Enable / disable an existing alert	1. Navigate to one of the following locations: • **Managed Objects** → **Active Directory** → **Real-Time Alerts** • **Managed Objects** → **Event Log** → **Real-Time Alerts** 2. Right-click an alert and select **Enable** or **Disable**.	1. Proceed to the **Configure Real-Time Alerts** step . 2. Double-click an alert to enable or disable it.
Modify an existing alert	1. Navigate to one of the following locations: • **Managed Objects** → **Active Directory** → **Real-Time Alerts** • **Managed Objects** → **Event Log** → **Real-Time Alerts** 2. Select an alert from the list in the left pane. 3. In the right pane, check **Enable** since only the enabled alerts can be modified. 4. Navigate to the options that require modification and update	1. Proceed to the **Configure Real-Time Alerts** step. 2. Select an alert and click **Edit**. The **Edit Real-Time Alert** wizard will open.

To..	In the Netwrix Auditor console	In the Managed Object wizard
	them.	
Create a new alert	1. Navigate to one of the following locations: • **Managed Objects** → **Active Directory** → **Real-Time Alerts** • **Managed Objects** → **Event Log** → **Real-Time Alerts** 2. Right-click the **Real-Time Alerts** node and select **New Real-Time Alert**. The **New Real-Time Alert** wizard will open.	1. Proceed to the **Configure Real-Time Alerts** step . 2. Click **Add**. The **New Real-Time Alert** wizard will open.

Review the following for additional information:

- Create Real-Time Alerts for Active Directory Auditing
- Create Real-Time Alerts for Event Log Management
- Create Real-Time Alerts for Mailbox Access Auditing via Event Log Management

The table below lists the predefined Real-Time Alerts, provided by Netwrix:

Alert	Description
Active Directory Auditing	
Changes to Admin Group Membership	Alerts on changes to the Domain Admins and the Enterprise Admins group
Changes to AD Objects by “Administrator”	Alerts on any changes to Active Directory objects made under the “administrator” account
Changes to Any Active Directory Objects	Alerts on any changes made to any Active Directory object
Changes to Domain Configuration	Alerts on changes to objects in domain configuration partition, such as sites, trusts, and so on
Domain Controller Demotion	Alerts on a domain controller demotion
Domain Controller	Alerts on a domain controller promotion

Alert	Description
Promotion	
Organizational Unit Deletion	Alerts on an Organizational Unit deletion
Event Log Management	
System Errors	Alerts on errors in the System event log
Application Errors	Alerts on errors in the Application event log

5.1. Create Real-Time Alerts for Active Directory Auditing

1. Start the **New Real-Time Alert** wizard. See Configure Real-Time Alerts for more information.
2. On the **Specify Real-Time Alert Name** step, specify the alert name and enter alert description (optional).
3. On the **Configure Real-Time Alert Filters and Notifications** step, specify the alert filters and configure email notifications. Click **Add** in the **Alert Filters** section to specify a condition that will trigger the alert.
4. Complete the **Alert Filter** wizard. Review the following for additional information:
   - In the **General** tab:

Option	Description
Name	Specify the filter name.
Description	Enter the description for this filter (optional).
Alert severity	Select alert severity level from the drop-down list (Critical / High / Normal / Low). **NOTE:** Alert severity level will be displayed in the email notification.

   - In the **Change** tab:

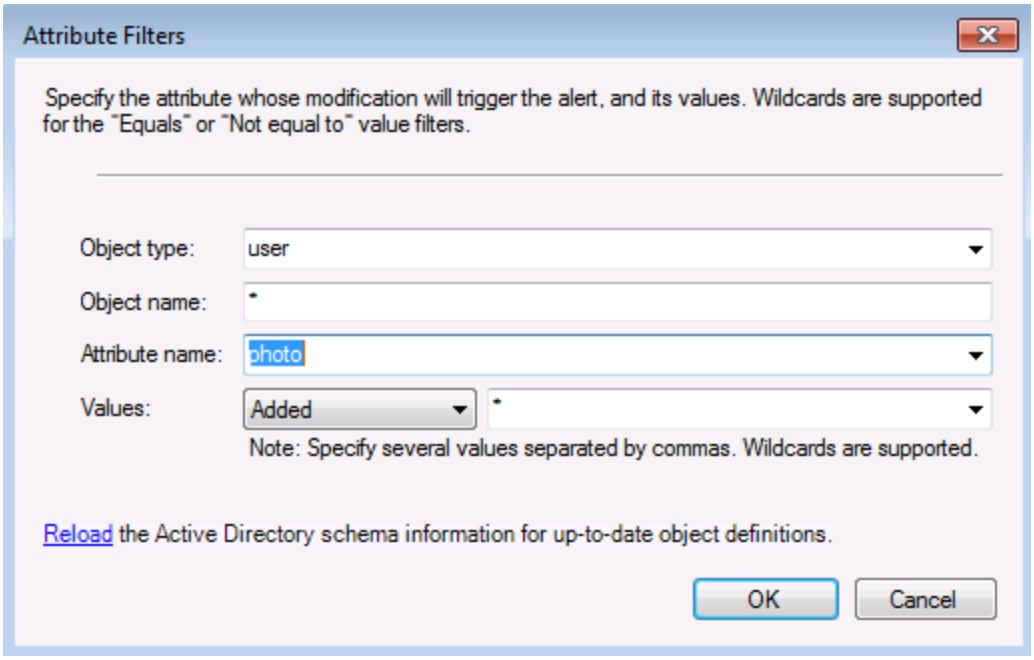
Option	Description
Who changed	Specify the name of the user whose actions must trigger the alert.

Option	Description
	Click  to select users from your domain. Alternatively, you can use a wildcard (*). In this case, the alert will be triggered if the action is performed by any user. If the product is configured to collect the information on group membership of the users who make changes, you can also select a group if you want to be notified when a change is made by any member of this group.
Change type	Select a change type (Add/Modify/Remove) from the drop-down list.
Object path	Specify the object path, i.e. the path to the AD object whose modification you want to track.
Include child objects	Select this option if you want the filter to be applied to all child objects in the specified path.

- In the **Attributes** tab, click **Add** to specify an AD object attribute whose modification must trigger the alert:

Option	Description
Object type	Select object type from the drop-down list. This list contains all Active Directory object types.
Object name	(Optional) Select object name to limit alerting to certain objects. You can use wildcard (*).
Attribute name	Select the attribute whose modification must trigger the alert. This list is populated depending on the selected object type.
Values	This field is displayed if a multi-value attribute is selected (e.g. "photo"). Select the type of change (e.g. Added or Removed), and specify the filter values.
Previous value	This field is displayed if a single-value attribute is selected. Select a value (possible values are: **Equals**, **Not equal to**, **Starts with**, **Ends with**, **Less than**, **Greater than**, **Less or equal**, **Greater or equal**) and specify the previous value of the attribute.

Option	Description
Current value	This field is displayed if a single-value attribute is selected. Select a value (possible values are: **Equals**, **Not equal to**, **Starts with**, **Ends with**, **Less than**, **Greater than**, **Less or equal**, **Greater or equal**) and specify the current value of the attribute.



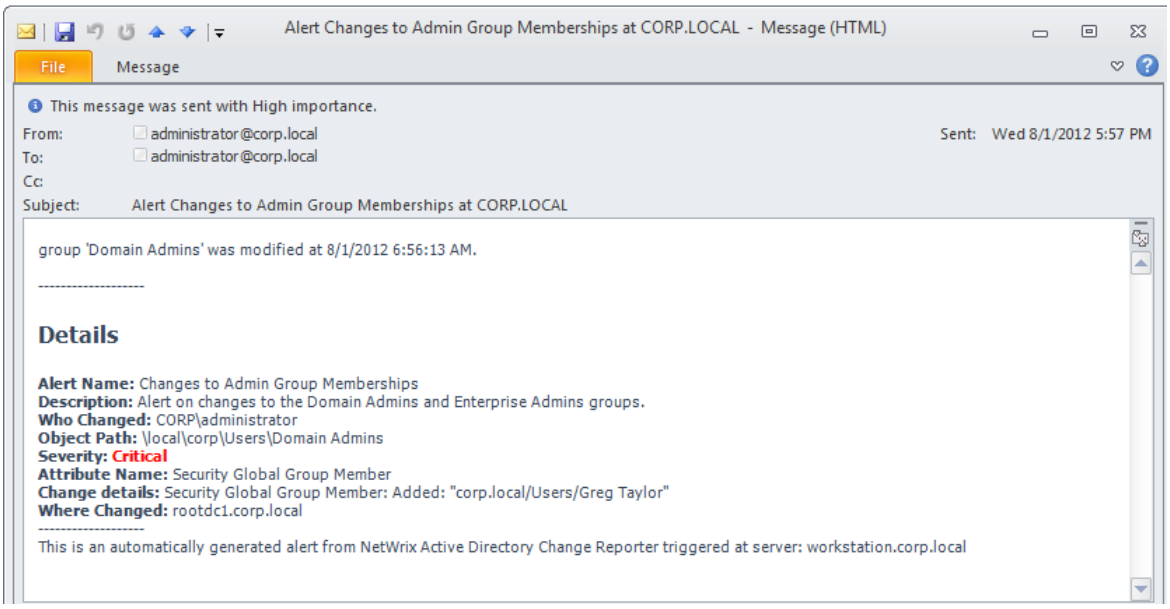
NOTE: Sometimes, it can be quite difficult to select the appropriate attribute for the type of change that must trigger an alert. If you are unsure which attribute is responsible for the type of change you want to track, refer to Identify Correct Attributes for detailed instructions on how to identify an attribute.

Click **OK** to save the changes and close the **Attribute Filters** dialog. And **OK** to save the changes and close the **Alert Filter** dialog.

5. In the **Notifications** section of the **New Real-Time Alert** wizard, click **Add** button and select **Email**. Specify the email address where notifications will be delivered. You can add as many recipients as necessary.

   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.

6. Review your Real-Time Alert settings and click **Finish** to exit the wizard. The new alert will be created under the **Real-Time Alerts** node. If an event occurs that triggers an alert, an email notification like in the example below will be sent immediately to the specified recipients:



Refer to the Netwrix Technical article for detailed instructions how to create some popular custom alerts ("User granted VPN permissions", "User account lockout").

5.1.1. Identify Correct Attributes

1. On the domain controller, make a test change that you want to configure a Real-Time Alert for and that will act as a trigger.
2. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** and click **Run** in the right pane. On data collection completion, you will receive a Change Summary email containing a list of changes that have been detected.
3. In this email, look for the parameter name in the **Details** column of the corresponding change.
4. Open the `propnames.txt` file located in the product installation folder and search for this parameter name. The value corresponding to this parameter is the name of the attribute you are looking for.

   NOTE: If you are unable to locate the parameter name in the `propnames.txt` file, that means that the Change Summary email contains the internal AD name for this attribute instead of a friendly name. In this case, this is the name of the attribute you are looking for that must be specified in the **Attribute Filters** dialog.

For example, if you want to create an alert that is triggered by modifications of a user's Dial-in/VPN permissions, and you are unsure which attribute is responsible for this change, do the following:

1. On the domain controller, navigate to **Start** → **Administrative Tools** → **Active Directory Users and Computers**.
2. Expand the domain node and select **Users**.
3. Right-click a user and select **Properties** from the pop-up menu.

4. In the **Dial-in** tab, select **Allow access** in the **Network Access Permission** section.
5. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** and click **Run** in the right pane. On data collection completion, you will receive a Change Summary email containing the change you have made.
6. In the **Details** column, locate the change parameter: **Allow Dial-in**.
7. Open the `propnames.txt` file and search for this parameter name. The entry in this file must say: `*.msNPAllowDialin=Allow Dial-In. "msNPAllowDialin"` is the name of the attribute that must be selected from the drop-down list in the **Attribute Filters** dialog when creating the alert.

5.2. Create Real-Time Alerts for Event Log Management

1. Start the **New Real-Time Alert** wizard. See Configure Real-Time Alerts for more information.
2. On the **Specify Real-Time Alert Properties** step, specify the alert name and enter alert description (optional). Specify the number alerts per email. Grouped alerts for different computers will be delivered in separate email messages. This value is set to 1 by default, which means that each alert will be delivered as a separate email message.
3. On the **Configure Real-Time Alert Filters and Notifications** step, specify the alert filters and configure email notifications. Click **Add** in the **Event Filters** section to specify an event that will trigger the alert.
4. Complete the **Event Filter** wizard. Review the following for additional information:
   - In the **Event** tab:

Option	Description
Name	Specify the filter name.
Description	Enter the description for this filter (optional).
Event Log	Select an event log from the drop-down list. You will be alerted on events from this event log. You can also input a different event log. To find out a log's name, navigate to **Start** → **Control Panel** → **Administrative Tools** → **Event Viewer** → **Applications and Services Logs** → **Microsoft** → **Windows** and expand the required **<Log_Name>** node, right-click the file under it and select **Properties**. Find the event log's name in the **Full Name** field. Netwrix Auditor does not collect the Analytic and Debug logs, so you cannot configure alerts for these logs.

Option	Description
	NOTE: You can use a wildcard (*). In this case you will be alerted on events from all Windows logs except for the ones mentioned above. Syslog events will be ignored.

- In the **Event Fields** tab:

Option	Description
Event ID	Enter the identifier of a specific event that you want to be alerted on. You can add several IDs separated by comma.
Event Level	Select the event types that you want to be alerted on. If the **Event Level** check-box is cleared, you will be alerted on all event types of the specified log.
Computer	Specify a computer. You will only be alerted on events from this computer. **NOTE:** If you want to specify several computers, you can define a mask for this parameter. Below is an example of a mask: • * - any machine • computer –a machine named 'computer' • *computer* - machines with names like 'xXxcomputerxXx' or 'newcomputer' • computer? – machines with names like 'computer1' or 'computerV' • co?puter - machines with names like 'computer' or 'coXputer' • ????? – any machine with a 5-character name • ???* - any machine with a 3-character name or longer
User	Enter a user's name. You will be alerted only on the events generated under this account. **NOTE:** If you need to specify several users, you can define a mask for this parameter in the same way as described above.
Source	Specify this parameter if you want to be alerted on the events from a specific source.

Option	Description
	NOTE: If you need to specify several users, you can define a mask for this parameter in the same way as described above.
Category	Specify this parameter if you want to be alerted on a specific event category.

- In the **Insertion Strings** tab:

Option	Description
Consider the following event Insertion Strings	Specify this parameter if you want to receive alerts on events containing a specific string in the EventData. You can use a wildcard (*). Click **Add** and specify **Insertion String**.

Click **OK** to save the changes and close the **Event Filters** dialog.

5. On the **Configure Real-Time Alerts Filers and Notifications** step of the **New Real-Time Alert** dialog, navigate to the **Notifications** section. Select **Events Summary recipients**, if you want the notifications to be delivered to the same email addresses as specified for Event Summaries. Alternatively, select **Specify recipients**, click **Add** and specify the email address where notifications will be delivered.

   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.

6. On the **Configure Real-Time Alerts Filers and Notifications** step, customize the notification template if needed. Click **Edit** next to **Customize notifications template**. Edit the template by deleting or inserting information fields.
7. Review your Real-Time Alert settings and click **Finish** to exit the wizard. The new alert will be created under the **Real-Time Alerts** node. If an event occurs that triggers an alert, an email notification like in the example below will be sent immediately to the specified recipients.

5.3. Create Real-Time Alerts for Mailbox Access Auditing via Event Log Management

Currently Mailbox Access Auditing does not provide a functionality to create real-time alerts. But you can configure real-time alerts to be triggered by non-owner mailbox access events (e.g. opening a message folder, opening/modifying/deleting a message, etc.) via Event Log Management.

To enable real-time alerts for Mailbox Access Auditing, you need to create a **Computer Collection** Managed Object for Event Log Management and configure the both features to work together.

Perform the following procedures:

- To create a Computer Collection Managed Object to audit logs on your Exchange Server
- To create a Real-Time Alert

To create a Computer Collection Managed Object to audit logs on your Exchange Server

NOTE: The procedure below describes the basic steps, required for creation of the Computer Collection Managed Object that will be used to collect data on non-owner mailbox access events. See Create Managed Objects for Event Log Management for more information.

1. Do one of the following:
   - In the Netwrix Auditor console main window select **Event Log**.
   - Select a **Computer Collection** as a Managed Object.

   See Managed Objects Overview for more information.
2. On the **Specify Computer Collection Name** step, enter the computer collection name.
3. On the **Configure Reports Settings** step, clear **Enable Reports**.
4. On the **Add Items to Computer Collection** step, select the **Windows Server** item type and add your Exchange Server.
5. On the **Specify Change Summary Recipients** step, do not provide email address to receive the summary as Mailbox Access Auditing will send daily emails.
6. On the **Configure Real-Time Alerts** step, disable predefined Real-Time Alerts.
7. On the **Configure Audit Archiving Filters** step, in **Inclusive Filters** section clear the filters you don't need, click **Add** and specify the following information:
   - The filter name and description (e.g. Mailbox Access Auditing)
   - In **Event Log**, enter *"Netwrix Non-owner Mailbox Access Agent"*.
   - In **Write to**, select **Audit Archive**. The events will be saved into the local repository.
8. 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.

To create a Real-Time Alert

1. Start the **New Real-Time Alert** wizard. See Configure Real-Time Alerts for more information.
2. On the **Specify Real-Time Alert Properties** step, specify the alert name and enter alert description (optional). Specify the number alerts per email. Grouped alerts for different computers will be delivered in separate email messages. This value is set to 1 by default, which means that each alert will be delivered as a separate email message.
3. On the **Configure Real-Time Alert Filters and Notifications** step, specify the alert filters and

configure email notifications. Click **Add** in the **Event Filters** section to specify an event that will trigger the alert.

4. Complete the **Event Filter** wizard. Review the following for additional information:

   - In the **Event** tab, specify the filter name and description. In the **Event Log** field enter *"Netwrix Non-owner Mailbox Access Agent"*.
   - In the **Event Fields** tab, complete the following fields:
     - Event ID—Enter the identifier of a specific event that you want to be alerted on. You can add several IDs separated by comma. Review the event IDs available in the Netwrix Non-owner Mailbox Access Agent event log:

ID	Description	Access Type (as displayed in XML view of event details)
1	A folder was opened	actFolderOpen
2	A message was opened	actMessageOpened
3	A message was sent	actMessageSubmit
4	A message was changed and saved	actChangedMessageSaved
5	A message was deleted	actMessageDeleted
6	A folder was deleted	actFolderDeleted
7	The entire contents of a folder was deleted	actAllFolderContentsDeleted
8	A message was created and saved	actMessageCreatedAndSaved
9	A message was moved or/and copied	actMessageMoveCopy
10	A folder was moved or/and copied	actFolderMoveCopy
14	A folder was created	actFolderCreated

     - Source—Enter *"Netwrix Non-owner Mailbox Access Agent"*.
   - In the **Insertion Strings** tab, select **Consider the following event Insertion Strings** to receive alerts on events containing a specific string in the EventData. Click **Add** and specify **Insertion String**.

   Click **OK** to save the changes and close the **Event Filters** dialog.

5. On the **Configure Real-Time Alerts Filers and Notifications** step of the **New Real-Time Alert**

dialog, navigate to the **Notifications** section. Select **Events Summary recipients**, select **Specify recipients**, click **Add** and specify the email address where notifications will be delivered. You can add as many recipients as necessary.

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.

6. On the **Configure Real-Time Alerts Filers and Notifications** step, customize the notification template if needed. Click **Edit** next to **Customize notifications template**. Edit the template by deleting or inserting information fields.
7. Review your Real-Time Alert settings and click **Finish** to exit the wizard. The new alert will be created under the **Real-Time Alerts** node. If an event occurs that triggers an alert, an email notification like in the example below will be sent immediately to the specified recipients.

5.3.1. Review Event Description

Depending on the event, the strings in the description may vary. The first eight strings are common for all events:

String	Description
String1	The event type: info or warning
String2	The event date and time in the following format: YYYY_MM_DD_hh_mm_ss_000
String3	The name of the user accessing mailbox
String4	The SID of the user accessing mailbox
String5	The GUID of the mailbox being accessed
String6	Shows whether the user accessing mailbox is the owner: it is always *false*
String7	The IP of the computer accessing the mailbox
String8	The access type

The following strings depend on the non-owner access type, represented by different Event IDs:

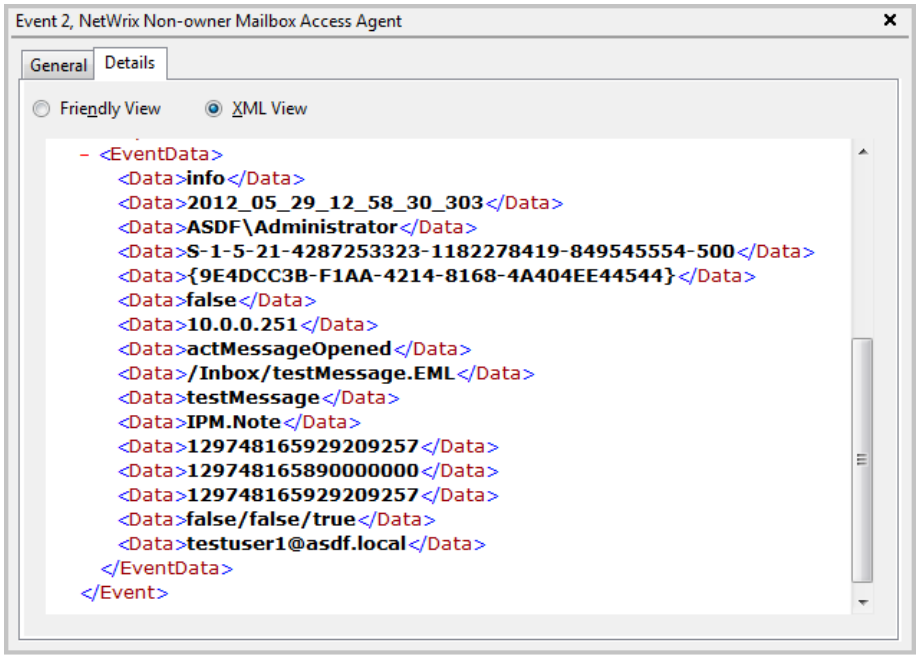
Event ID	Access type (String 8)	Strings	Description
1	actFolderOpen	String9	The internal folder URL

Event ID	Access type (String 8)	Strings	Description
2	actMessageOpened	String9	The internal folder URL
		String10	The message subject
		String11	The message type: IPM.Note – Email, IPM.Contact – contact, etc.
3	actMessageSubmit	String9	The internal folder URL
		String10	The message subject
		String11	Email addresses of the message recipients, separated by a semicolon
		String12	The message type: IPM.Note – Email, IPM.Contact – contact, etc.
4	actChangedMessageSaved	String9	The internal folder URL
		String10	The message subject
		String11	The message type: IPM.Note – Email, IPM.Contact – contact, etc.
5	actMessageDeleted	String9	The internal folder URL
		String10	The message subject
		String11	The message type: IPM.Note – Email, IPM.Contact – contact, etc.
6	actFolderDeleted	String9	The internal folder URL
7	actAllFolderContentsDeleted	String9	The internal folder URL
8	actMessageCreatedAndSaved	String9	The internal folder URL
9	actMessageMoveCopy	String9	The message being moved/copied – the final part of the message URL, e.g. /Inbox/testMessage.EML
		String10	The action – copy or move
		String11	The folder URL the message is copied/moved from

Event ID	Access type (String 8)	Strings	Description
		String12	The destination folder URL
		String13	The message type: IPM.Note – Email, IPM.Contact – contact, etc.
10	actFolderMoveCopy	Strings 9 -13	The string descriptions for the folder are the similar to those for messages.
14	actFolderCreated	String9	The new folder URL

NOTE: With different Exchange Server versions and/or different email clients (Outlook 2003, 2007, 2010, OWA), the same non-owner action (e.g. copying a message) may generate different events: e.g. **actMessageMoveCopy** with one server/client or **actMessageCreatedAndSaved** with another.

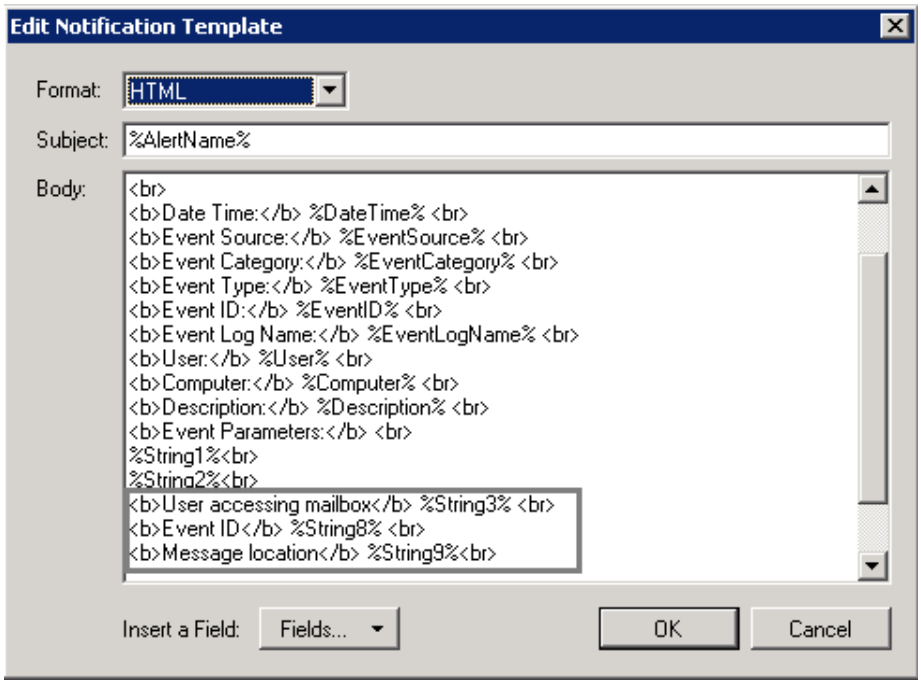
Below you can see an example of the MessageOpened event in the XML view.



You can add the required strings contained in % symbols for your own custom alert separated by a `<br>` tag in `<b>Event Parameters:</b>`. Event parameter descriptions can also be added.

In the example below, the following information has been added:

- The description for String 3– User accessing mailbox
- String 8 with the description
- String 9 with the description


Edit Notification Template
Format:
HTML
Subject:
%AlertName%
Body:

Date Time: %DateTime%
Event Source: %EventSource%
Event Category: %EventCategory%
Event Type: %EventType%
Event ID: %EventID%
Event Log Name: %EventLogName%
User: %User%
Computer: %Computer%
Description: %Description%
Event Parameters:
%String1%
%String2%
User accessing mailbox %String3%
Event ID %String8%
Message location %String9%
Insert a Field:
Fields...
OK
Cancel

6. Configure Global Settings

The Netwrix Auditor console provides a convenient interface for configuring or modifying settings that are applied to all existing Managed Objects and all target systems audited with the product. This chapter provides detailed instructions on how to configure these settings.

NOTE: For instructions on how to configure or modify the settings for Managed Objects individually, or the target system audited with the product, refer to Modify Managed Objects.

To modify global settings

1. In the Netwrix Auditor console, navigate to **Settings**.
2. In the right pane, click on the setting name to see details. Review the following for additional information:
   - Configure Reports Settings
   - Configure Email Notifications Settings
   - Configure Audit Archive Settings
   - Configure Data Collection Settings
   - Configure Syslog Platforms Settings
   - Configure Netwrix Console Audit
   - Update Licenses

6.1. Configure Reports Settings

The default settings are configured when you create the first Managed Object and enable the Reports functionality in the **New Managed Object** wizard. If you have not specified the default Reports settings before, navigate to **Settings** → **Reports** and click **Configure** to launch the **Reports Configuration** wizard.

If you have the Reports functionality configured, review information on your default SQL Server database used to store audit data and generate SSRS-based reports and modify it if necessary. Click **Modify** to update report settings. Click **Apply** to apply these settings to all Managed Objects (custom reports settings will be overwritten).

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.

Refer to Configure Reports for detailed instructions on how to configure reports functionality.

6.2. Configure Email Notifications Settings

Review the default SMTP settings used to deliver email notifications, reports, etc. or click **Modify** to adjust them.

Setting	Description
SMTP server	Enter your SMTP server name.
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.

Setting	Description
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.

6.3. Configure Audit Archive Settings

Review and update the Audit Archive location and the retention period for the local repository of audit data. Click **Modify** to configure these settings.

Setting	Description
Write audit data to	Specify the path to the folder where your audit data will be stored.
Retention period for audit data (in months)	Specify the number of months for which audit data will be stored. Data will be deleted automatically when its retention period is over. If the retention period is set to *0*, data will be stored for the last 4 sessions.
Retention period for Sessions (in days)	Specify the number of days for which Sessions (i.e. the information on daily data collection status) are stored and are available for review in the Netwrix Auditor console. **NOTE:** The Session retention period does not affect the Audit Archive retention settings.

6.4. Configure Data Collection Settings

Review the default data collection settings, including the default Data Processing Account and data collection schedule, and update it if necessary.

To modify default data collection and Change Summary generation schedule

1. Click **Modify** next to **Default data collection and Change Summary generation schedule**.
2. In the **Modify Schedule** dialog, set the new schedule (for example, increase the number of data collections per day or the start time).
    - You can also create several scheduled tasks to collect data. To do it, select **Show multiple schedules**. After selecting this check-box you will be able to expand the scheduled tasks list and

create new tasks and modify them separately.

- Click **Advanced** to customize your scheduled data collection task. In the **Advanced Schedule Options** dialog, you can specify the **Start** and the **End** dates, frequency, task duration, etc.

To modify the default Data Processing Account

1. Click **Modify** next to **Default Data Processing Account**.
2. Provide the account credentials.

NOTE: Make sure that the new account is granted all required rights and permissions to collect data from the monitored computers. Refer to Netwrix Auditor Installation and Configuration Guide for more information.

6.5. Configure Syslog Platforms Settings

NOTE: This topic describes functionality that can be used within the Event Log Management feature only.

To display a list of currently available Syslog-based platforms, in the Netwrix Auditor console, navigate to **Syslog Platforms** under the **Settings** node. Netwrix Auditor provides the following predefined platform types: Generic, Red Hat Enterprise Linux 5, and Ubuntu.

You can also create and configure new Syslog-based platforms that can be subsequently selected as item types for your Managed Objects.

The following operations are supported:

- Contact Netwrix Support to order a custom platform from Netwrix if the predefined platforms do not cover your needs.
- Click **Add** to add a new platform. See To create a Syslog-based platform for more information.
- Select a platform from the list and click **Edit** to modify it.

  NOTE: You cannot edit a predefined platform. If you try to edit it, a copy of this platform will be created, which can be modified.
- Select a custom platform and click **Remove** to delete a platform.

  NOTE: the predefined platforms cannot be deleted.
- Click **View** to view platform rules.
- Click **Modify** next to **Syslog server port** to update a port number.

To create a Syslog-based platform

1. Click **Add**.
2. In the **New Syslog Platform** dialog, select the following parameters:

- Select the platform type. Select **New** to create a new platform and define its rules. Alternatively, you can select **Copy**, and create a platform based on a predefined platform, thus inheriting its rules and edit it afterwards.
- Specify a platform name and add a description.

3. On the next step, click **Add** to add events processing rules. You can also edit, re-order and delete rules on this step. To store events that do not match any of the rule patterns, select the corresponding check-box.
4. In the dialog that opens, specify the following parameters:

Parameter	Description
Enable	Make sure that this option is selected.
Rule name	Specify the rule name.
Description	Specify the rule description (optional).
Regular expression pattern	Specify a pattern, according to which events will be collected. When an event matches this pattern, this event will be logged. The rows below contain information that will be added to a Syslog event if it matches a specified pattern. This information can be used to filter events and sort them by.
Source	Specify the name of a source. It can be any word that will help you identify the platform where an event was generated.
User name	Specify the number of a capturing group which defines a user name in a pattern in the following format: `%Capturing_Group_Number`. If needed, you can add more information, for example: `Domain_Name\%Capturing_Group_Number`. The right `Capturing_Group_Number` can be calculated if you enumerate capturing groups in a pattern starting from *0*.
Event ID	Specify a number which will be added to an event as its ID.
Event level	Specify the event level.

5. Review the details and complete the wizard. The platform will be added to the **Available platforms** list.

NOTE: To view reports for the predefined platforms, there are default report templates located in *%Netwrix Auditor installation folder%/Event Log Manager/Reports/Netwrix Event Log Manager/Best Practice Reports/Syslog*. To view reports for custom platforms, you can use report templates

located in *%Netwrix Auditor installation folder%/Event Log Manager/Reports/Netwrix Event Log Manager/General Reports*.

6.6. Configure Netwrix Console Audit

The Netwrix Console Audit option allows you to keep record of any actions made via the Netwrix Auditor console and audit changes to Managed Objects configuration, auditing settings, common settings, etc. This functionality is available if the User Activity Video Recording feature is enabled. It allows capturing video of any activity on the audited computers and embedding metadata (such as the information on which applications and windows were opened) into video files, which can be used for data search and positioning inside video recordings.

To enable Netwrix Console Audit

1. In the Netwrix Auditor console, expand the **Settings** node and select **Netwrix Console Audit**.
2. Click **Configure**. A Managed Object called Netwrix Console Audit will be created automatically with the following default settings:

Parameter	Value
Audited System	User Activity
Monitored Computers	localhost
Filter by user	All users
Filter by application	Netwrix*
Reports	Not configured
Automatic Activity Summary Delivery	Not configured
Video recording quality and duration settings	Default

To view an Activity Summary showing the actions performed in the Netwrix Auditor console, navigate to **Managed Objects** → **Netwrix Console Audit** → **User Activity** → **Activity Records**.

To enable automatic Activity Summary delivery navigate to **Managed Objects** → **Netwrix Console Audit** → **User Activity**. Click **Configure Delivery** and in the dialog that opens specify the delivery schedule and the target email address.

You can modify the Netwrix Console Audit settings (for example, enable SSRS-based Reports, adjust video quality settings, etc.) in the same way as for any other Managed Object. See Modify Managed Objects for more information.

6.7. Update Licenses

The Licenses node allows you to review the status of your current licenses, update them and add new licenses.

To update/add a license

1. Click **Update Licenses**.
2. In the dialog that opens, do one of the following:

- Select the **Load from file** option, click Browse and point to a license file received from your sales representative.
- Select the **Enter manually** option and type in your company name, license count and license codes.

7. Roll Back Unwanted Changes In Your IT Infrastructure

7.1. Roll Back Changes With Active Directory Object Restore

With Netwrix Auditor you can quickly restore deleted and modified objects using the Active Directory Object Restore tool integrated with the product. This tool enables AD object restore without rebooting a domain controller and touching the rest of the AD structure, and goes beyond the standard tombstone capabilities.

Perform the following procedures:

- Modify Schema Container Settings
- Roll Back Unwanted Changes

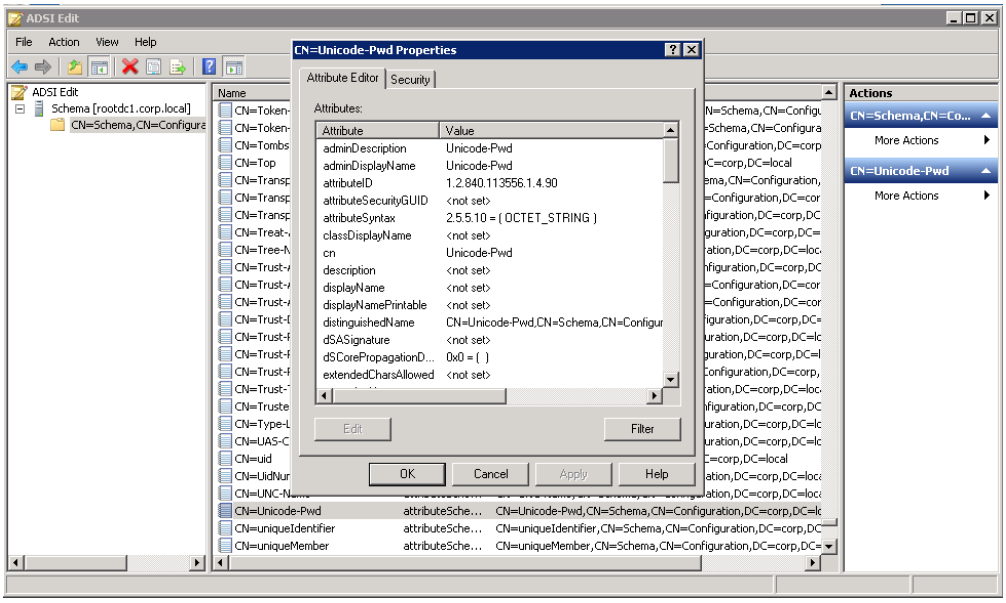
7.1.1. Modify Schema Container Settings

By default, when a user or computer account is deleted from Active Directory, its password is discarded. When you restore deleted accounts with the Active Directory Object Restore tool, it sets random passwords which then have to be changed manually. If you want to be able to restore AD objects with their passwords preserved, you need to modify the Schema container settings so that account passwords are retained when accounts are deleted.

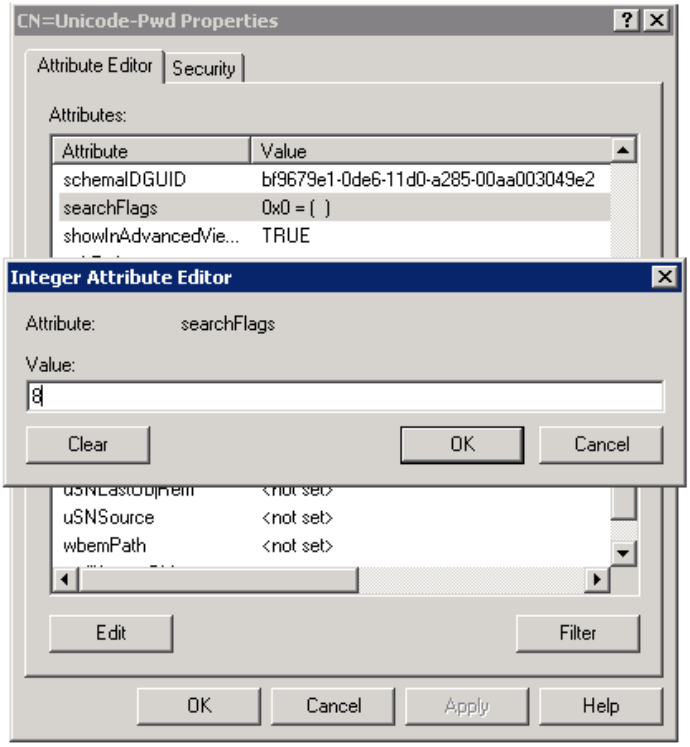
To modify schema container settings

NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2003 systems, this utility is a component of Windows Server Support Tools. In Windows Server 2008 systems and above, this component is installed together with the AD DS role, or it can be downloaded and installed along with Remote Server Administration Tools.

1. Navigate to **Start** → **Programs** → **Administrative Tools** → **ADSI Edit**.
2. Right-click the **ADSI Edit** node and select **Connect To**. In the **Connection Settings** dialog, enable **Select a well-known Naming Context** and select **Schema** from the drop-down list.
3. Expand the **Schema <Your_Root_Domain_Name>** node. Right-click the **CN=Unicode-Pwd** attribute and select **Properties**.



4. Double-click the **searchFlags** attribute and set its value to *"8"*.



Now you will be able to restore deleted accounts with their passwords preserved.

7.1.2. Roll Back Unwanted Changes

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Active Directory**.
2. In the right pane, click **Restore AD Objects** next to **Active Directory Object Restore**.

3. On the **Select Rollback Period** step, specify the period of time when the changes that you want to revert occurred. You can either select a period between a specified date and the present date, or between two specified dates.
4. On the **Select Rollback Source** step, specify the rollback source and monitored domain. The following restore options are available:
   - **Restore from state-in-time snapshots** — This option allows restoring objects from configuration snapshots made by Netwrix Auditor. This option is more preferable since it allows to restore AD objects with all their attributes.

     You can select the **Select a state-in-time snapshot** option if you want to revert to a specific snapshot. Otherwise, the program will automatically search for the most recent snapshot that will cover the selected time period.
   - **Restore from AD tombstones**—This option is recommended when no snapshot is available. This is a last resort measure as the tombstone holds only the basic object attributes.
5. On the **Analyzing Changes** step, the product analyzes the changes made during the specified time period. When reverting to a snapshot, the tool reviews the changes that occurred between the specified snapshots. When restoring from a tombstone, the tool reviews all AD objects put in the tombstone during the specified period of time.
6. On the **Select Changes to Roll Back** step, the analysis results are displayed. Select a change to see its rollback details in the bottom of the window. Select an attribute and click **Details** to see what changes will be applied if this attribute is selected for rollback. Check the changes you want to roll back to their previous state.
7. Wait until the tool has finished restoring the selected objects. On the last step, review the results and click **Finish** to exit the wizard.

7.2. Restore Group Policy Objects

With Netwrix Auditor, you can restore your Group Policy objects via the backup files saved by the product. The backups are stored in the folder with snapshots and event log information, the default path is: *%ProgramData%\Netwrix\Management Console\Data\AD Changes\<domain_name>*.

You can use this feature after at least one data collection task has run.

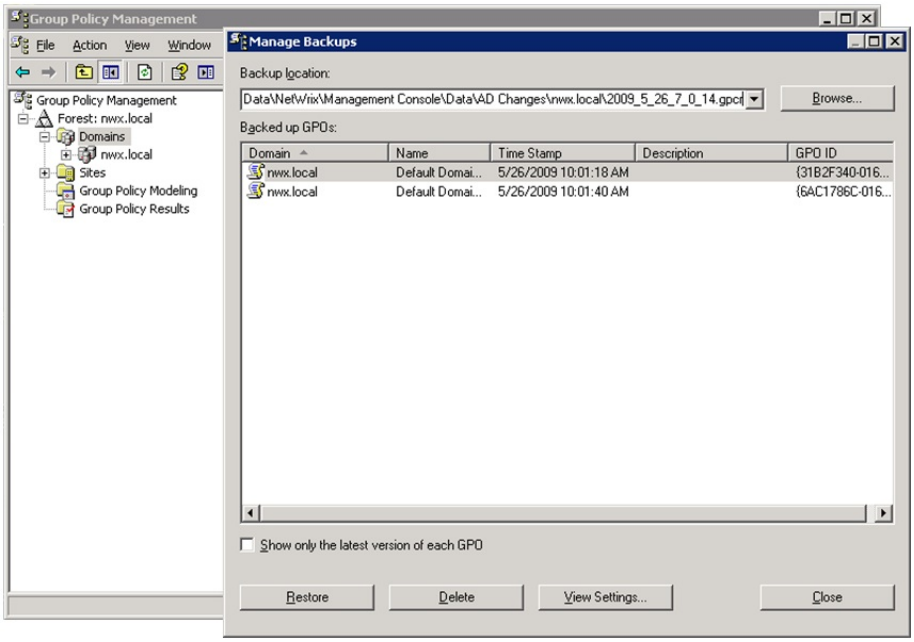
NOTE: By default, backup files are not saved. To enable saving, set the **GPOBackup** registry key value to *"1"*. See Registry Keys in Group Policy Auditing for more information.

To restore Group Policy objects

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. Expand the **Forest: <your_forest_name>** node, right-click **Domains** and select **Manage Backups**

from the drop-down menu.

3. In the **Manage Backups** dialog, click **Browse** and select the folder with Group Policy backup files. The folders with backup files are usually named by dates, so you can pick a folder by the required date. You will be presented with a list of Group Policy objects backed up on the selected date.



4. Select the Group Policy object you want to restore and click **Restore**.

7.3. Roll Back Changes With Windows File Server Auditing

Enable the **Enable file versioning and rollback capabilities** option to create rollback points based on the Volume Shadow Copy technology. This is a built-in service in Windows XP and above. For detailed information on the Volume Shadow Copy Service, refer to Microsoft documentation.

If any data, file or permission is changed or deleted, you will always be able to perform a rollback of these actions.

Perform the following procedures:

- Configure Volume Shadow Copy Service
- Enable File Versioning And Roll Back Capabilities
- Restore Your File System

7.3.1. Configure Volume Shadow Copy Service

You can configure the maximum size of your shadow copies storage. To do this, perform the following procedure:

1. Navigate to the volume that you want to create shadow copies for.
2. Right-click it and select **Properties**, and navigate to the **Shadow Copies** tab.
3. Click **Settings**.
4. In the **Settings** dialog, select **Use limit** and specify your storage maximum size.

   NOTE: By default, the maximum size is set to *10* percent of the source volume being copied. For recommendations on how to select a correct size limit for your shadow copies storage, refer to section "Amount of volume space to allocate to shadow copies" of the following article provided by Microsoft: Designing a Shadow Copy Strategy.

7.3.2. Enable File Versioning And Roll Back Capabilities

NOTE: The file shares that you want to create shadow copies for must have been included in the Computer collection items list in your Managed Objects. See Create Managed Objects for Windows File Server Auditing for more information.

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **File Servers.**
2. In the right pane, select **Enable file versioning and rollback capabilities**.

   Alternatively, you can enable this option under **Advanced** on the **Configure File Server Change Reporter Settings** step of the **New Managed Object** wizard.

Every time Netwrix Auditor runs a data collection task (by default, every 24 hours, at 3 AM), it will create a shadow copy of your file system that you can roll back to at any time.

7.3.3. Restore Your File System

If unwanted changes have been made to your file system, perform the following procedure to roll back to a point created by Netwrix Auditor:

1. Navigate to the network share that changes have been made to and that you want to restore.
2. Right-click the folder, select **Properties** and navigate to the **Previous Versions** tab. A list of all shadow copies with the date and time when they were created will be displayed.
3. Select a shadow copy you want to roll back to and click **Open**. A snapshot of your file system for the selected date will be displayed.

   NOTE: You can roll back to the selected backup point using a variety of tools. The examples in this guide use a built-in Windows utility called **Robocopy**.

4. Launch the **Robocopy** utility. To do this,navigate to **Start** → **Run** and type *"robocopy"*.

5. Depending on the type of changes you want to roll back, enter the command into the program's command prompt, similar to the following:

   - To restore files that have been removed from your monitored share:

     Enter the path to the source network share (i.e the shadow copy created by the system), the path to the destination (i.e. your network share that you want to restore) and the 'DAT' command in the following format: `"<source_path>" "<destination_path>" /copy:dat`

     Example:

     ```
     "\\localhost\C$\@GMT-2011.09.27-12.24.25\test" "C:\test" /copy:dat
     ```

   - To restore your file system if file security or audit permissions have been changed:

     Enter the path to the source network share (i.e the shadow copy created by the system), the path to the destination (i.e. your network share that you want to restore) and the 'SOU' and 'SECFIX' commands in the following format: `"<source_path>" "<destination_path>" /copy:sou /secfix`

     Example:

     ```
     "\\localhost\C$\@GMT-2011.09.27-12.24.25\test" "C:\test" /copy:sou /SECFIX
     ```

6. As a result, your file share will be reverted to the selected backup point.

8. Additional Configuration

This chapter provides instructions on how to fine-tune Netwrix Auditor using the additional configuration options. Review the following for additional information:

- Enable Monitoring of Active Directory Partitions
- Configure Audit Archiving Filters
- Exclude Objects From Auditing Scope
- Fine-tune Netwrix Auditor Using Registry Keys
- Enable Integration with Third-Party SIEM Solutions

8.1. Enable Monitoring of Active Directory Partitions

NOTE: This topic corresponds to the Active Directory Auditing feature.

Active Directory environment consists of the following three directory partitions:

- **Domain partition** stores users, computers, groups and other objects. Updates to this partition are replicated only to domain controllers within the domain.
- **Configuration partition** stores configuration objects for the entire forest. Updates to this partition are replicated to all domain controllers in the forest. Configuration objects store the information on sites, services, directory partitions, etc.
- **Schema partition** stores class and attribute definitions for all existing and possible Active Directory objects. Updates to this partition are replicated to all domain controllers in the forest.

By default, Netwrix Auditor only monitors changes to the Domain partition and the Configuration partition of the audited domain. If you also want to monitor changes to the Schema partition, or to disable monitoring of changes to the Configuration partition do the following:

NOTE: You cannot disable monitoring of changes to the Domain partition.

To enable monitoring of the Configuration and Schema partitions

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** → **Active Directory.**
2. In the right pane, click **Configure** next to **Advanced Options**.
3. In the Advanced Options dialog, select **Configuration** and **Schema**.

Information on changes to the selected partition(s) will be available in Reports and will be saved in snapshots.

8.2. Configure Audit Archiving Filters

NOTE: Currently this functionality is available in Event Log Management only.

Audit archiving filters define which events will be saved into the Audit Archive and/or a SQL database (if the **Reports** feature is enabled). You can enable/disable and modify existing filters and create new filters in one of the following locations:

- Configure audit archiving filters while creating a Managed Object for Event Log Management. See Create Managed Objects for Event Log Management for more information.
- If you have a Managed Object configured to audit your logs with Event Log Management, proceed with following steps. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_ Managed_Object>** → **Event Log** → **Audit Archiving Filters**.

Netwrix Auditor allows creating inclusive and exclusive audit archiving filters.

To configure audit archiving filters, perform the following operations:

- To create or modify an audit archiving filter, refer to To create or edit an audit archiving filter.
- To collect events required to generate a specific report, you must select a filter whose name coincides with this report's name. Click **Enable** and select **Filters for Reports**. All filters required to store events for all available reports will be selected automatically.
- To select filters required to collect events for regulatory compliances (GLBA, HIPAA, PCI, SOX), click **Enable**, click **Select compliance** and choose the required regulation.

To create or edit an audit archiving filter

1. On the **Audit Archiving Filters** page, click **Add** or select a filter and click **Edit**.
2. Complete the fields. Review the following for additional information:

Option	Description
	The **Event** tab
Name	Specify the filter name.
Description	Enter the description for this filter (optional).
Event Log	Select an event log from the drop-down list. You will be alerted on events from this event log. You can also input a different event log. To find out a log's name, navigate to **Start** → **Control Panel** → **Administrative Tools** → **Event Viewer** → **Applications and Services Logs** → **Microsoft** → **Windows** and expand the required **<Log_Name>** node, right-click the file under it and select

Option	Description
	Properties. Find the event log's name in the **Full Name** field. Netwrix Auditor does not collect the Analytic and Debug logs, so you cannot configure alerts for these logs. By selecting the **Syslog** option, the events from Syslog-based platforms only will be processed. Events from custom Windows logs with the same names will not be collected. **NOTE:** You can use a wildcard (*). For inclusive filters: all Windows logs except for the ones mentioned above will be saved. Syslog events will be ignored. For exclusive: all Windows logs events will be excluded. Syslog events will be stored.
Write to/Don't write to	Select the location to write/not to write events to, depending on the filter type (inclusive or exclusive). **NOTE:** It is recommended to write the same events to the Audit Archive and to a SQL database, because if your database is corrupted, you will be able to import the necessary data from the Audit Archive using the Database Importer tool. See To import audit data to a SQL database for more information.
	The **Event Fields** tab
Event ID	Enter the identifier of a specific event that you want to be save. You can add several IDs separated by comma.
Event Level	Select the event types that you want to be save. If the Event Level check box is cleared, all event types will be saved. **NOTE:** If your monitored computers run Windows Vista and above and you want to select the inclusive **Success Audit/Failure Audit** filters, note that on these platforms these events belong to the "Information" level, so they will not be collected if you select the **Information** check-box in the **Exclusive Filters**.
Computer	Specify a computer. Only events from this computer will be saved. **NOTE:** If you want to specify several computers, you can define a mask for this parameter. Below is an example of a mask:

Option	Description
	• * - any machine • computer – a machine named 'computer' • *computer* - machines with names like 'xXxcomputerxXx' or 'newcomputer' • computer? – machines with names like 'computer1' or 'computerV' • co?puter - machines with names like 'computer' or 'coXputer' • ????? – any machine with a 5-character name • ???* - any machine with a 3-character name or longer
User	Enter a user's name. Only events created by this user will be saved. **NOTE:** If you need to specify several users, you can define a mask for this parameter in the same way as described above.
Source	Specify this parameter if you want to save events from a specific source. **NOTE:** If you need to specify several sources, you can define a mask for this parameter in the same way as described above.
Category	Specify this parameter if you want to save a specific events category.
	The **Insertion Strings** tab
Consider the following event Insertion Strings	Specify this parameter if you want to store events containing a specific string in the EventData. You can use a wildcard (*). Click **Add** and specify **Insertion String**.

8.3. Exclude Objects From Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the auditing scope. This can be helpful if you want to reduce time required for the data collection, reduce the disk space, required to store the collected data and customize the reports.

To exclude data from the auditing scope, perform the following procedures:

- Exclude Data From Active Directory Auditing Scope
- Exclude Data From Group Policy Auditing Scope

- Exclude Data From Exchange Server Auditing Scope
- Exclude Data From Mailbox Access Auditing Scope
- Exclude Data From Windows File Server, NetApp Filer and EMC Storage Auditing Scope
- Exclude Data From Windows Server Auditing Scope
- Exclude Data From Event Log Management Scope
- Exclude Data From Inactive User Tracking Scope
- Exclude Data From Password Expiration Alerting Scope
- Exclude Data From SQL Server Auditing Scope
- Exclude Data From SharePoint Auditing Scope
- Exclude Data From VMware Auditing Scope

8.3.1. Exclude Data From Active Directory Auditing Scope

You can fine-tune Active Directory Auditing by specifying data that you want to exclude from the auditing scope.

To exclude data from Active Directory Auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\AD Change Reporter Full Version* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
addprops.txt	Allows adding properties to appear in the Change Summaries for newly created AD objects. When a new object is added, Netwrix Auditor does not show any data in the **Details column** in the Change Summary emails. If you want to see the information on certain attributes of a newly created	`Object type:property:` For example, to show a group description on this group's creation, add the following line: `group:description:`

File	Description	Syntax
	object, specify these attributes in this file.	

allowedpathlist.txt	Contains a list of AD paths to be included in change reports.
	
	This file can be used, for example, if you only want to monitor specific OU(s) inside your AD domain, but not the entire domain. In this case, put a wildcard (*) in the omitpathlist.txt file to exclude all paths, and then specify the OU(s) you want to monitor in the **allowedpathlist.txt** file.
		`Path`
		
		NOTE: The path must be in the format displayed in the **Object Name** column in the Change Summary or the **What Changed** column in SSRS-based Reports.
		
		For example, to monitor only the **Users** OU in domain **CORP**, add the following line:
		
		`\local\corp\Users\*`
		
		In the omitpathlist.txt file, specify the wildcard (*)

omitallowedpathlist.txt	Contains a list of AD paths to be excluded from Change Summaries and Reports.
	
	This file can be used if you want to exclude certain paths inside those specified in the allowedpathlist.txt file. In this case, put a wildcard (*) in the omitpathlist.txt file to exclude all paths, then specify the OU(s) you want to monitor in the allowedpathlist.txt file, and then specify the paths you want to exclude from within them in the **omitallowedpathlist.txt** file.
		`Path`
		
		NOTE: The path must be in the format displayed in the **Object Name** column in the Change Summary or the **What Changed** column in SSRS-based Reports.
		
		For example, to monitor the **Users** OU, but to exclude users **jsmith** and **pbrown**, do the following:
		
		1. Add the wildcard (*) to the **omitpathlist.txt** file.
		2. Add the following line to the **allowedpathlist.txt** file: `*\Users\*`
		3. Add the following lines to the **omitallowedpathlist.txt** file:
		
		`*\pbrown`
		
		`*\jsmith`

omitobjlist.txt	Contains a list of object types to be excluded from	`Object type` For example, to omit changes to the

File	Description	Syntax
	change reports.	**printQueue** object, add the following line: `printQueue`.
omitpathlist.txt	Contains a list of AD paths to be excluded from change reports.	`Path` **NOTE:** The path must be in the format displayed in the **Object Name** column in the Change Summary or the **What Changed** column in SSRS-based Reports. For example, to exclude changes to the **Service Desk** OU, add the following line: `*\Service Desk\*`.
omitproplist.txt	Contains a list of object types and properties to be excluded from change reports.	`object_type.property_name` **NOTE:** If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example to exclude the **adminCount** property from Reports, add the following line: `*.adminCount`.

omitreporterrors.txt	Contains a list of errors to be excluded from Change Summaries.	`Error message text`
		
		For example, if you have granular audit settings applied to your domain controllers policy, the following error will be returned in the Change Summary emails:
		
		`Auditing of Directory Service Access is not enabled for this DC. Adjust the audit policy settings using the Active Directory Audit Configuration Wizard or see the product documentation for more information.`
		
		Add the text of this error message to this file to stop getting it in the Change Summary emails.

File	Description	Syntax
omitsnapshotpathlist.txt	Contains a list of AD paths to be excluded from AD snapshots.	`Path` **NOTE:** The path must be in the format displayed in the **Object Name** column in the Change Summary or the **What Changed** column in SSRS-based Reports. For example, to exclude data on the **Disabled Accounts** OU from the the **Snapshot** report, add the following line: `*\Disabled Accounts*`.
omitstorelist.txt	Contains a list of object types and properties to be excluded from AD snapshots.	`object_type.property_name` **NOTE:** If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example to exclude data on the AD **adminDescription** property, add the following line: `*.adminDescription`.
processaddedprops.txt	Allows adding properties to appear in change reports (SSRS-based) for newly created AD objects. When a new object is created, Netwrix Auditor does not show any data in the **Details** column in reports. If you want to see the information on certain attributes of a newly created object, specify these attributes in this file.	`object type:property:` For example, if you want a user's **Description** property to be displayed in the reports when a user is added, add the following line: `User:Description:`
processdeletedprops.txt	Allows adding properties to appear in change reports (SSRS-based) for deleted AD objects. When an object is deleted, Netwrix Auditor does not show any data in	`object type:property:` For example, if you want a user's **Description** property to be displayed in the reports when a user is deleted, add the following line: `User:Description:`

File	Description	Syntax
	the **Details** column in reports. If you want to see the information on certain attributes of a deleted object, specify these attributes in this file.	
propnames.txt	Contains a list of human-readable names for object types and properties to be displayed in change reports.	`classname.attrname=intelligiblename` For example, if you want the **adminDescription** property to be displayed in the reports as **Admin Screen Description**, add the following line: `*.adminDesciption=Admin Screen Description`

8.3.2. Exclude Data From Group Policy Auditing Scope

You can fine-tune Group Policy Auditing by specifying data that you want to exclude from the auditing scope. To do it, edit the **omitobjlist_gp.txt**, **omitproplist_gp.txt** and **omituserlist_gp.txt** files.

To exclude data from Group Policy Auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\AD Change Reporter Full Version* folder.
2. Edit **omitobjlist_gp.txt**, **omitproplist_gp.txt** and **omituserlist_gp.txt** files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcard (*) is supported and can be used to replace any number of characters.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitobjlist_gp.txt	The file contains a list of the Group Policy Object (GPO) names to be excluded from change reports.	`<object name>` For example, to exclude changes to the Default Domain Policy GPO, add the following line: `Default Domain Policy`.
omitproplist_gp.txt	The file contains a list of the Group Policy Object settings to be	`<settingname>`

File	Description	Syntax
	excluded from change reports.	For example, to exclude data on changes made to the Maximum password length setting, add the following line: `Maximum password length`.
omituserlist_gp	The file contains a list of user names to be excluded from change reports.	`<domain\user>` For example, to exclude changes made by the user "usertest" in the domain "domaintest", add the following line: `domaintest\usertest`.

8.3.3. Exclude Data From Exchange Server Auditing Scope

You can fine-tune Exchange Server Auditing by specifying data that you want to exclude from the auditing scope.

To exclude data from Exchange Server Auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\AD Change Reporter Full Version* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

aal_omitlist.txt	For Exchange Server 2010 and above, the file contains a list of changes performed by cmdlets. To exclude a change from reports, specify name of a cmdlet and the attribute that is changed by the selected cmdlet.	`cmdlet.attrname`
		For example:
		`Set-User`
		`Set-ContactSet-Group`
		`#Update-AddressList`
		`Add-ADPermissionRemove-ADPermission`
		`#RBAC:`
		`*-MailboxAuditLogSearch`

File	Description	Syntax
		`*-AdminAuditLogSearch`

aal_propnames.txt	For Exchange Server 2010 and above, the file contains a list of human-readable names of changed attributes to be displayed in change reports. To exclude a change from the reports, specify name of a cmdlet and the attribute that is changed by the selected cmdlet.	`classname.attrname=intelligiblename`
		For example:
		`*- OutlookAnywhere.SSLOffloading = Allow secure channel (SSL) offloading`

omitobjlist_ecr.txt	Contains a list of human-readable names of object classes to be excluded from change reports.	`Classname`
		For example:
		`exchangeAdminService`
		`msExchMessageDeliveryConfig`
		`Exchange_DSAccessDC`

omitpathlist_ecr.txt	Contains a list of AD paths to be excluded from change reports.	`Path`
		For example:
		`*\Microsoft Exchange System Objects\SystemMailbox*`

omitproplist_ecr.txt	Contains a list of object types and properties to be excluded from change reports.	`object_type.property_name`
		NOTE: If there is no separator (.) between an object type and a property, the whole entry is treated as an object type.
		For example:
		`msExchSystemMailbox.*`
		`*.msExchEdgeSyncCredential`
		`*.msExchMailboxMoveTargetMDBLink`
		`*.adminDescription`

omitreporterrors_ecr.txt	Contains a list of errors to be excluded from Change Summaries.	`Error message text` For example, to omit the error "The HTTP service used by Public Folders is not

File	Description	Syntax
		available, possible causes are that Public stores are not mounted and the Information Store service is not running. ID no: c1030af3", add `*c1030af3*` to the file.

omitserverlist_ecr.txt	Defines the Exchange 2003 servers to be excluded from data collection.	`NetBIOS_server_name`
		For example:
		`Exchangesrv01`

omitexchangeserverlist.txt	Defines the Exchange 2010 and 2013 servers to be excluded from data collection.	`FQDN_server_name`
		For example:
		`Exchangeserv01.enteprise.local`

omitstorelist_ecr.txt	Contains a list of classes and attributes names to be excluded from MS Exchange snapshots.	`object_type.property_name`
		NOTE: If there is no separator (.) between an object type and a property, the whole entry is treated as an object type.
		For example:
		`Exchange_ Server.AdministrativeGroup`
		`Exchange_ Server.AdministrativeNote`
		`Exchange_Server.CreationTime`

propnames_ecr2003.txt	Contains a list of human-readable names for object types and properties of Exchange 2003 to be displayed in change reports.	`classname.attrname=intelligiblename`
		For example:
		`###WMI / AD (Common)`
		`Exchange_Mailbox = Mailbox`
		`Exchange_ Mailbox.StorageLimitInfo = Storage Limit Info`

propnames_ecr2007.txt	Contains a list of human-readable names for object classes and attributes of	`classname.attrname=intelligiblename` For example:

File	Description	Syntax
	Exchange 2007 to be displayed in change reports.	`msExchMDBAvailabilityGroup = Database Availability Group`

8.3.4. Exclude Data From Mailbox Access Auditing Scope

Netwrix Auditor allows specifying users and mailboxes that you do not want to monitor with the Mailbox Access Auditing feature. To do this, edit the **mailboxestoexclude.txt**, **userstoexclude.txt**, and **agentomitusers.txt** files.

To exclude users or mailboxes from the Mailbox Access Auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\Non-owner Mailbox Access Reporter for Exchange* folder.
2. Edit **mailboxestoexclude.txt**, **userstoexclude.txt**, or **agentomitusers.txt** files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (* and ?) are supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description
mailboxestoexclude.txt	This file contains a list of mailboxes and folders that must be excluded from reports. You can specify a 'Mailbox_Name', a 'Mailbox_Name/Folder_Name', or use wildcards (*/Folder_Name). In the last example, the specified folder will be excluded in all mailboxes. If agents are disabled, the 'Mailbox_Name/Folder_Name' lines are ignored.
userstoexclude.txt	This file contains a list of users who must be excluded from reports if they perform non-owner access to mailboxes (audit data on these users will still be stored in the snapshots). If a user is removed from this list, the information on this user's actions can be viewed with the Report Viewer.
agentomitusers.txt	This file contains a list of users who must be excluded from reports and snapshots. If a user is removed from this list, audit data on this user will only be

File	Description
	available after the next data collection. Writing new users to this file affect reports and snapshots only if **Use agents to collect detailed audit data** is enabled.

8.3.5. Exclude Data From Windows File Server, NetApp Filer and EMC Storage Auditing Scope

You can fine-tune Windows File Server, NetApp Filer and EMC Storage Auditing by specifying data that you want to exclude from the auditing scope.

To exclude data from Windows File Server, NetApp Filer and EMC Storage Auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\File Server Change Reporter* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitobjlist.txt	Contains a list of object types to be excluded from change reports.	`Object type`
omitpathlist.txt	Contains a list of UNC paths to be excluded from change reports.	`UNC_Path`
omitproplist.txt	Contains a list of attributes' names to be excluded from change reports.	`Attribute_name`
omitstorelist.txt	Contains a list of objects the information on those will be excluded from saving to the Audit Archive.	`UNC_Path`
omitstoreproplist.txt	Contains a list of attributes the information on those will	`Attribute_name`

File	Description	Syntax
	be excluded from saving to the Audit Archive.	
omitstoreuserlist_fs.txt	Contains a list of users information on whose will be excluded from saving to the Audit Archive.	`domain\username`
omituserlist_fs.txt	Contains a list of users to be excluded from change reports.	`domain\username`
propnames.txt	Contains a list of human-readable names for object types and properties to be displayed in change reports.	`object_type_name.attribute_name=friendlyname` For example, if you want the path to the shared folder to be displayed in the reports as **Local Path**, add the following line: `*.Share Path=Local Path`

8.3.6. Exclude Data From Windows Server Auditing Scope

You can fine-tune Windows Server Auditing by specifying data that you want to exclude from the auditing scope.

To exclude data from the Windows Server Auditing reports

1. Navigate to the *%Netwrix Auditor install folder%\Windows Server Change Reporter* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (* and ?) are supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitdblist.txt	Contains a list of objects to be excluded from SSRS-based Reports.	`Managed Object name,who changed,server name,object type,resource path,property name` **NOTE:** A backslash (\) must be put in front of (*) and (?) if they are part of an entry value.

File	Description	Syntax
		For example: `*,productionserver1.corp.local,*,*,*,StartTimeLo (REG_DWORD)`

omitreportist.txt	Contains a list of objects to be excluded from Change Summary emails.	`Managed Object name,who changed,server name,object type,resource path,property name`
		NOTE: A backslash (\) must be put in front of (*) and (?) if they are part of an entry value.
		For example:
		`*,CORP\\jsmith,*,*,*,*`

omitstorelist.txt	Contains a list of objects to be excluded from Change Summary emails.	`Managed Object name,server name,class name,property name,property value`
		NOTE: A backslash (\) must be put in front of (*) and (?) if they are part of an entry value.
		For example:
		`*,*,StdServerRegProv,name,HKEY_LOCAL_MACHINE\\COMPONENTS`

omiterrors.txt	Contains a list of errors/warnings to be omitted from Change Summary emails or Session details.	`Managed Object Name,server name,error text`
		NOTE: A backslash (\) must be put in front of (*) and (?) if they are part of an entry value.
		For example:
		`*,productionserver1.corp.local,Auditing of registry keys is not enabled for this server`

8.3.7. Exclude Data From Event Log Management Scope

You can fine-tune Event Log Management by specifying data that you want to exclude from the auditing scope.

To exclude data from the Event Log Management scope

1. Navigate to the *%Netwrix Auditor install folder%\Event Log Manager* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (* and ?) are supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitErrorsList.txt	Contains a list of data collection errors and warnings to be excluded from reports.	`Error text`

omitLogErrorList.txt	Contains a list of event log names and servers to be excluded from the reports if errors or warnings were returned on data collection.	`server\event log name`
		For example:
		`*\DNS*`

omitServerList.txt	Contains a list of server names or servers IP addresses to be excluded from Event Log Management processing.	`ip address` or `server name`
		For example:
		`192.168.3.*`

omiterrors.txt	Contains a list of errors/warnings to be omitted from Change Summary emails or Session details.	`Managed Object Name,server name,error text`
		NOTE: A backslash (\) must be put in front of (*) and (?) if they are part of an entry value.
		For example:
		`*,productionserver1.corp.local,Auditing of registry keys is not enabled for this server`

8.3.8. Exclude Data From Inactive User Tracking Scope

You can fine-tune Inactive User Tracking by specifying data that you want to exclude from the auditing scope.

To exclude data from the Inactive User Tracking auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\Inactive Users Tracker Full Version* folder.
2. Edit the **omitdclist.txt** file, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (* and ?) are supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitdclist.txt	Contains a list of domain controllers to be excluded from processing. The Inactive User Tracking feature skips all automated deactivation actions (disable, move, delete) even if one domain controller is unavailable during scheduled task execution. Add the unavailable domain controllers to this file to ensure Inactive User Tracking functions properly.	`Full DNS name` or `NetBIOS name` **NOTE:** IP addresses are not supported.

8.3.9. Exclude Data From Password Expiration Alerting Scope

You can fine-tune Password Expiration Alerting by specifying data that you want to exclude from the auditing scope.

To exclude data from the Password Expiration Alerting auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\Password Expiration Notifier* folder.
2. Edit the **omitoutlist.txt** file, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcard (*) is supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitdclist.txt	Contains a list of Organizational Units to be excluded from processing.	`Path`
		For example:
		`*OU=C,OU=B,OU=A*`

8.3.10. Exclude Data From SQL Server Auditing Scope

You can fine-tune SQL Server Auditing by specifying data that you want to exclude from the auditing scope.

To exclude data from the SQL Server Auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\SQL Server Change Reporter* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcard (*) is supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitobjlist.txt	Contains a list of object types to be excluded from the reports.	`Object type`
		For example:
		`Database`
		`Column`

omitpathlist.txt	Contains a list of resource paths to the objects to be excluded from the reports.	`Server_instance:resource_path` where `resource_path` is shown in the **Resource Name** column in the reports. For example, to exclude information about databases whose names start with "tmp" on the SQL Server instance "PROD.SQL2008": `PROD.SQL2008:Databases\tmp*`.
omitproplist.txt	Contains a list of attributes to be excluded from change reports.	`object_type_name.property_name.attribute_name` where: • `object_ type_ name` — Can be

File	Description	Syntax
		found in the **Resource Type** column in change reports. • `property_name`—Can be found in the **Details** column (property name is bold). • `attribute_name`—Can be found in the **Details** column (attribute name is not bold). If an object does not have an attribute name, use the ***** character. For example to exclude information about the **Size** attribute of the **Database File** property in all databases: `Database.Database File.Size`.
omitstorelist.txt	Contains a list of objects the information on those will be excluded from saving to the Audit Archive.	`server_instance.resource_path` where`resource_path` is shown in the **Resource Name** column in the reports.
omittracelist.txt	Excludes **Who changed** and **When changed** data of certain SQL Server instances from the reports.	`server\instance name`

pathtotracelogs.txt	Contains a list of SQL Server instances whose traces must be stored locally.	`SQLServer\Instance|UNC path`
		For example:
		`server\instance|C:\Program Files\Microsoft SQL Server\MSSQL\LOG\`

propnames.txt	Contains a list of human-readable names for object types and properties to be displayed in the change reports.	`object_type_name.attribute_name=friendlyname`
		For example:
		`*.Date modified=Modification Time`

8.3.11. Exclude Data From SharePoint Auditing Scope

You can fine-tune SharePoint Auditing by specifying data that you want to exclude from the auditing scope.

To exclude data from SharePoint Auditing scope

1. Navigate to the *%ProgramData%\Netwrix\Netwrix Auditor for SharePoint\Configuration\<Managed_Object_Name>* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcard (*) is supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitscstorelist.txt	Contains a list of site collections to be excluded from audit data collection.	`http(s)://URL`
		NOTE: Enter the root web site URLs.
		If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for different zones, you can use any of these URLs to specify a child site collection.
		For example:
		`https://siteColl*`

omitwastorelist.txt	Contains a list of web applications to be excluded from audit data collection.	`http(s)://URL`
		NOTE: Enter the root web site URLs.
		If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for different zones, you can use any of these URLs.
		For example:
		`http://webApplication1:3333/`

File	Description	Syntax

omiteventloglist.txt	Contains a list of event IDs to be excluded from the Event Log.
	
	NOTE: Only add known error or warning events, otherwise you may lose important data.
		`event ID`
		
		For example:
		
		`1001`

8.3.12. Exclude Data From VMware Auditing Scope

You can fine-tune VMware Auditing by specifying various data types that you want to exclude/include from/in the reports.

To exclude data from VMware Auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\Change Reporter for VI3 Full Version* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitproplist.txt	Contains a list of object types and properties to be excluded from change reports.	`object_type.property_name` **NOTE:** If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example, to exclude the **config.flags.monitorType** property from reports, add the following line: `*.config.flags.monitorType`.
hidepropvalues.txt	Contains a list of object types and properties to be excluded from the reports when the property is set to certain	`object_type.property_name=property_value:object_type.hidden_property` For example, to exclude the **config.cpuAllocation.shares.level** property when

File	Description	Syntax
	value.	it equals to *"Low"*, add the following line: `*.config.cpuAllocation.shares.level=low:*.config.cpuAllocation.shares.shares.`
proplist.txt	Contains a list of human-readable names for object types and properties to be displayed in the reports.	`inner_type:object_type.property=intelligiblename` **NOTE:** `Inner_type` is optional. For example, if you want the **configStatus** property to be displayed in the reports as **Configuration Status**, add the following line: `*.configStatus=Configuration Status.`

8.4. Fine-tune Netwrix Auditor With Registry Keys

You can fine-tune Netwrix Auditor using the Registry keys as described below. This functionality is currently available for the following Netwrix Auditor features:

- Registry Keys in Active Directory Auditing
- Registry Keys in Group Policy Auditing
- Registry Keys in Exchange Server Auditing
- Registry Keys in Windows File Server Auditing
- Registry Keys in Inactive User Tracking
- Registry Keys in Event Log Management
- Registry Keys in Windows Server Auditing

8.4.1. Registry Keys in Active Directory Auditing

Review the basic Active Directory Auditing registry keys that you may need to configure while using the product. Navigate to **Start** → **Run** and type *"regedit"*.

Registry key	Type	Description / Value	Created during setup	Pre-served during upgrade
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432NODE)\Netwrix\AD Change Reporter\<Managed Object name>\ Database Settings				

Registry key	Type	Description / Value	Created during setup	Pre-served during upgrade
SessionIncrementalUpdate	REG_ DWORD	Defines whether to perform incremental update for database statistics on each data collection: • 0—No • 1—Yes	No (Created when Snapshot Reportin g feature is enabled for this Managed Object)	No
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\AD Change Reporter				
CleanAutoBackupLogs	REG_ DWORD	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours	Yes	Yes
IgnoreAuditCheckResultError	REG_ DWORD	Defines whether audit check errors should be displayed in the Change Summary footer: • 0—Display errors • 1—Do not display errors	Yes	Yes
IgnoreRootDCErrors	REG_ DWORD	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Change Summary footer: • 0—Display errors • 1—Do not display errors	Yes	Yes

Registry key	Type	Description / Value	Created during setup	Pre-served during upgrade
MonitorModifiedAndRevertedBack	REG_DWORD	Defines whether the Change Summary must display the attributes whose values were modified and then restored between data collections: • 0—These attributes are not displayed • 1—These attributes are displayed as "modified and reverted back"	No	No
ShortEmailSubjects	REG_DWORD	Defines whether to contract the email subjects (e.g. Netwrix Active Directory Change Reporter: Summary Report – ADCR Report): • 0—No • 1—Yes	No	Yes
ProcessBackupLogs	REG_DWORD	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.	Yes	Yes
ShowReportFooter	REG_DWORD	Defines whether to display the footer in the Change Summary email: • 0—No	Yes	Yes

Registry key	Type	Description / Value	Created during setup	Pre-served during upgrade
		• 1—Yes		
ShowReportGeneratorServer	REG_ DWORD	Defines whether to display the report generation server in the Change Summary footer: • 0—No • 1—Yes	Yes	Yes
ShowSummaryInFooter	REG_ DWORD	Defines whether to display the summary in the Change Summary footer: • 0—No • 1—Yes	Yes	Yes
ShowSummaryInHeader	REG_ DWORD	Defines whether to display the summary in the Change Summary header: • 0—No • 1—Yes	Yes	Yes
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\AD Change Reporter\<Managed Object Name>				
CollectLogsMaxThreads	REG_ DWORD	Defines the number of Domain Controllers to simultaneously start log collection on.	No	Yes
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\Management Console\Database settings				
overwrite_datasource	REG_ DWORD	Defines whether to overwrite the database connection settings (stored in the reports data source) if they differ from the SQL server settings specified when configuring the	No	Yes

Registry key	Type	Description / Value	Created during setup	Pre-served during upgrade
		Managed Object: • 0—No • 1—Yes		
SqlOperationTimeout	REG_ DWORD	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).	No	Yes
timeout	REG_ DWORD	Defines the SQL database connection timeout (in seconds).	No	Yes

8.4.2. Registry Keys in Group Policy Auditing

Review the basic Group Policy Auditing registry keys that you may need to configure while using the product. Navigate to **Start** → **Run** and type *"regedit"*.

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\AD Change Reporter				
CleanAutoBackupLogs	REG_ DWORD	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours	Yes	Yes
GPOBackup	REG_ DWORD	Defines whether to backup GPOs during data collection: • 0—No • 1—Yes	Yes	Yes

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
GPOBackupDays	REG_ DWORD	Defines the backup frequency: • 0—Backup always • X—Once in X days **NOTE:** GPOBackup must be set to *"1"*.	Yes	Yes
IgnoreAuditCheckResultError	REG_ DWORD	Defines whether audit check errors should be displayed in the Change Summary footer: • 0—Display errors • 1—Do not display errors	Yes	Yes
IgnoreRootDCErrors	REG_ DWORD	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Change Summary footer: • 0—Display errors • 1—Do not display errors	Yes	Yes
ShortEmailSubjects	REG_ DWORD	Defines whether to contract the email subjects (e.g. Netwrix Group Policy Change Reporter: Summary Report – GPCR Report): • 0—No • 1—Yes	No	Yes
ProcessBackupLogs	REG_ DWORD	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will	Yes	Yes

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
		not be deleted regardless of the value of the **CleanAutoBackupLogs** key.		
ShowReportFooter	REG_ DWORD	Defines whether to display the footer in the Change Summary email: • 0—No • 1—Yes	Yes	Yes
ShowReportGeneratorServer	REG_ DWORD	Defines whether to display the report generation server in the Change Summary footer: • 0—No • 1—Yes	Yes	Yes
ShowSummaryInFooter	REG_ DWORD	Defines whether to display the summary in the Change Summary footer: • 0—No • 1—Yes	Yes	Yes
ShowSummaryInHeader	REG_ DWORD	Defines whether to display the summary in the Change Summary header: • 0—No • 1—Yes	Yes	Yes
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\AD Change Reporter\<Managed Object Name>				
CollectLogsMaxThreads	REG_ DWORD	Defines the number of Domain Controllers to simultaneously start log collection on.	No	Yes
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\ AD Change Reporter\<Managed Object Name>\Database settings				

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
SessionImportDays	REG_ DWORD	Defines the frequency of a full snapshot upload: • X—Once in X days	No	Yes
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\Management Console\Database settings				
overwrite_datasource	REG_ DWORD	Defines whether to overwrite the database connection settings (stored in the reports data source) if they differ from the SQL server settings specified when configuring the Managed Object: • 0—No • 1—Yes	No	Yes
SqlOperationTimeout	REG_ DWORD	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).	No	Yes
timeout	REG_ DWORD	Defines the SQL database connection timeout (in seconds).	No	Yes

8.4.3. Registry Keys in Exchange Server Auditing

Review the basic Exchnage Server Auditing registry keys that you may need to configure while using the product. Navigate to **Start** → **Run** and type *"regedit"*.

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\AD Change Reporter				
CleanAutoBackupLogs	REG_ DWORD	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain	Yes	Yes

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
		controllers • [X]— Backups are deleted after [X] hours		
IgnoreAuditCheckResultError	REG_ DWORD	Defines whether audit check errors should be displayed in the Change Summary footer: • 0—Display errors • 1—Do not display errors	Yes	Yes
IgnoreRootDCErrors	REG_ DWORD	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Change Summary footer: • 0—Display errors • 1—Do not display errors	Yes	Yes
MonitorModifiedAndRevertedBack	REG_ DWORD	Defines whether the Change Summary must display the attributes whose values were modified and then restored between data collections: • 0—These attributes are not displayed • 1—These attributes are displayed as "modified and reverted back"	No	No
ShortEmailSubjects	REG_ DWORD	Defines whether to contract the email subjects (e.g. Netwrix Exchange Server Change Reporter: Summary Report – ECR Report): • 0—No • 1—Yes	No	Yes

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
ProcessBackupLogs	REG_ DWORD	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.	Yes	Yes
ShowReportFooter	REG_ DWORD	Defines whether to display the footer in the Change Summary email: • 0—No • 1—Yes	Yes	Yes
ShowReportGeneratorServer	REG_ DWORD	Defines whether to display the report generation server in the Change Summary footer: • 0—No • 1—Yes	Yes	Yes
ShowSummaryInFooter	REG_ DWORD	Defines whether to display the summary in the Change Summary footer: • 0—No • 1—Yes	Yes	Yes
ShowSummaryInHeader	REG_ DWORD	Defines whether to display the summary in the Change Summary header: • 0—No	Yes	Yes

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
		• 1—Yes		
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\AD Change Reporter\<Managed Object Name>				
CollectLogsMaxThreads	REG_ DWORD	Defines the number of Domain Controllers to simultaneously start log collection on.	No	Yes
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\Management Console\Database settings				
overwrite_datasource	REG_ DWORD	Defines whether to overwrite the database connection settings (stored in the reports data source) if they differ from the SQL server settings specified when configuring the Managed Object: • 0—No • 1—Yes	No	Yes
SqlOperationTimeout	REG_ DWORD	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).	No	Yes
timeout	REG_ DWORD	Defines the SQL database connection timeout (in seconds).	No	Yes

8.4.4. Registry Keys in Event Log Management

Review the basic Event Log Management registry keys that you may need to configure while using the product. Navigate to **Start** → **Run** and type *"regedit"*.

Registry key	Type	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\Netwrix\Event Log Manager\<Managed Object		

Registry key	Type	Description / Value
Name>\Database Settings		
Ar_enabled	REG_ DWORD	Defines the Reports functionality status: • 0—Disabled • 1—Enabled
ConnectionTimeout	REG_ DWORD	Defines SQL database connection timeout (in seconds).
HKEY_LOCAL_MACHINE\SOFTWARE\Netwrix\Event Log Manager\<Managed Object Name>\ElmDbOptions		
BatchSize	REG_ DWORD	Defines the number of entries processed in a batch (must be more than 1000).
BatchTimeOut	REG_ DWORD	Defines batch writing timeout (in seconds).
DeadLockErrorCount	REG_ DWORD	Defines the number of write attempts to a SQL database.
HKEY_LOCAL_MACHINE\SOFTWARE\Netwrix\Event Log Manager\<Managed Object Name>		
CleanAutoBackupLogs	REG_ DWORD	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
IgnoreRootDCErrors	REG_ DWORD	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Change Summary footer: • 0—Display errors • 1—Do not display errors
ProcessBackupLogs	REG_ DWORD	Defines whether to process security log backups: • 0—No • 1—Yes

Registry key	Type	Description / Value
		NOTE: Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.
WriteAgentsToApplicationLog	REG_ DWORD	Defines whether to write the events produced by the agent to the Application Log of a monitored machine: • 0—Disabled • 1—Enabled
WriteToApplicationLog	REG_ DWORD	Defines whether to write events produced by Netwrix Auditor to the Application Log of the machine where the product is installed: • 0—No • 1—Yes

8.4.5. Registry Keys in Inactive User Tracking

Review the basic Inactive User Tracking registry keys that you may need to configure while using the product. Navigate to **Start** → **Run** and type *"regedit"*.

Registry key	Type	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\Inactive Users Tracker		
WriteEventLog	REG_ DWORD	Defines whether to write events to the Application Log: • 0—No • 1—Yes

8.4.6. Registry Keys in Windows Server Auditing

Review the basic Windows Server Auditing registry keys that you may need to configure while using the product. Navigate to **Start** → **Run** and type *"regedit"*.

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\Windows Server Change Reporter				
CleanAutoBackupLogs	REG_ DWORD	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours	Yes	Yes
ProcessBackupLogs	REG_ DWORD	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.	Yes	No

8.4.7. Registry Keys in Windows File Server Auditing

Review the basic Windows File Server Auditing registry keys that you may need to configure while using the product. Navigate to **Start** → **Run** and type *"regedit"*.

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\Netwrix\File Server Change Reporter				
CleanAutoBackupLogs	REG_ DWORD	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted	Yes	Yes

Registry key	Type	Description / Value	Created during setup	Preserved during upgrade
		after [X] hours		
ProcessBackupLogs	REG_ DWORD	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.	Yes	No

8.5. Enable Integration with Third-Party SIEM Solutions

If your organization is already using a third-party Security Information and Event Management (SIEM) solution, Netwrix Auditor can help protect these investments by integrating with major SIEM systems. Netwrix Auditor allows you to manage audit data in your usual way, but with improved performance and increased reliability of the collected audit data.

The Active Directory Auditing, Group Policy Auditing and Exchange Server Auditing features within Netwrix Auditor can integrate with all major SIEM solutions, including:

- Microsoft System Center Operations Manager (SCOM) 2007 R2 and 2012
- RSA enVision®
- Arc-Sight® Logger™
- Novell® Sentinel™
- NetIQ® Security Manager™
- IBM Tivoli® Security Information
- Event Manager™
- and many others.

When integration with SIEM products is enabled, a custom Windows event log called Netwrix Change Reporter is created. This event log will generate events for each detected change. You can configure custom processing rules, alerts and reports in your SIEM solution to track these events.

8.5.1. Enable Integration

1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_Managed_Object>** . Depending on the feature you want to integrate with SIEM solution select corresponding node: **Active Directory** or **Group Policy** or **Exchange Server**.
2. In the right pane, select **Configure** next to **Advanced Options**.
3. In the **Advanced Options** dialog that opens, select **Microsoft System Center** to integrate the product with Microsoft SCOM and/or **Third-party SIEM products** to integrate the product with a different SIEM solution.
4. Depending on the SIEM solution you use, do one of the following:
   - **SCOM**—Download and install Netwrix SCOM Management Pack for change auditing and compliance. This solution allows SCOM to capture events written by Netwrix Auditor into a dedicated event log and generate corresponding reports and alerts. For detailed description of the alerts triggered by SCOM alerting rules, refer to SCOM Alerts .
   - Any other SIEM solution—Customize your solution to use the **Newtrix Change Reporter** event log and create rules to trigger alerts on certain events. Review the Netwrix event types and their structure below.

8.5.2. Netwrix Event Types

There are two categories of the Netwrix Change Reporter events:

- Audit events—These events contain the information on data collection. See Audit Events for more information.
- General Events—These events contain the information on errors that occurred during data collection, messages on successful data collection, and other general data. See General Events for more information.

Property	Audit event	General event
Source	• Netwrix Active Directory Change Reporter—Corresponds to the Active Directory Audting feature withing Netwrix Auditor. • Netwrix Group Policy Change Reporter—Corresponds to the Group Policy Audting feature withing Netwrix Auditor. • Netwrix Exchange Change Reporter—Corresponds to the Exchange Server Audting feature withing Netwrix Auditor.	
Category	Audit (id=1)	General (id=2)
Level	Success Audit / Failure Audit	Information / Warning / Error
ID	1001 – 1008	2001 - 2013

To review event properties

1. On the domain controller, navigate to **Start** → **Administrative Tools** → **Event Viewer**.
2. In the right pane, locate the **Netwrix Change Reporter** event log and double-click it.
3. Double-click an event.
4. In the **Event Properties** dialog, select one of the following tabs:
   - The **Event Properties General** tab shows the event description in the upper grid and the general properties information below the grid.
   - The **Details** tab shows the event details.

8.5.2.1. Audit Events

The table below provides a description of the audit events sorted by their ID.

ID	Name	Description	Change type string in description	Change detail string in description	Source
1001	Add	Object added	Added	—	• Netwrix Active Directory Change Reporter • Netwrix Group Policy Change Reporter • Netwrix Exchange Change Reporter
1002	Remove	Object removed	Removed	—	• Netwrix Active Directory Change Reporter • Netwrix Group Policy Change Reporter • Netwrix Exchange Change Reporter
1003	Modify	Single-valued string was modified. Empty values reported as empty quoted strings in description templates	Modified	<attribute > changed from “<old value>” to “<new value>”	• Netwrix Active Directory Change Reporter • Netwrix Group Policy Change Reporter • Netwrix Exchange Change Reporter

ID	Name	Description	Change type string in description	Change detail string in description	Source
1004	Modify by Events	Information extracted from Windows Event Log. (e.g. user account enabled/disabled, account locked/unlocked)	Modified	<attribute >	• Netwrix Active Directory Change Reporter • Netwrix Exchange Change Reporter
1005	Value Added	Value was added to the multi-valued attribute (e. g. a new member was added to a group)	Modified	<attribute>: Added: "<new value>"	• Netwrix Active Directory Change Reporter • Netwrix Exchange Change Reporter
1006	Value Removed	Value was removed from the multi-valued attribute, (e. g. a member was removed from a group)	Modified	<attribute >: Removed: "<old value>"	• Netwrix Active Directory Change Reporter • Netwrix Exchange Change Reporter
1007	Modified and Reverted Back	Attribute was modified and then rolled back to its previous value. Intermediate values are unknown.	Modified	<attribute >: Modified and Reverted back	• Netwrix Active Directory Change Reporter • Netwrix Exchange Change Reporter
1008	Access	Access to file system objects (e.g. successful or failure file reads; failure attempts to access a folder or share)	Read	—	

NOTE: (Group Policy Auditing) The Add/Remove events (Event ID 1001 or 1002) are generated only when a Group Policy object is added or removed. Changes to policy settings are always displayed as the Modified event (ID 1003).

The table below provides a description of the insertion strings that are displayed in the **Details** tab of the **Event Properties** dialog:

String number	Generic content	Active Directory Auditing	Exchange Server Auditing	Group Policy Auditing
Event Source Name	Product name	Netwrix Active Directory Change Reporter	Netwrix Exchange Change Reporter	Netwrix Group Policy Change Reporter
1	Managed Object	Domain	Domain	Domain
2	When detected (local)	-//-	-//-	-//-
3	When detected (UTC)	-//-	-//-	-//-
4	When changed (local)	-//-	-//-	-//-
5	When changed (UTC)	-//-	-//-	-//-
6	The name of the user who made the change (DOMAIN\user)	-//-	-//-	-//-
7	Object type	AD object type (computer/user/ group, etc.)	AD object type (computer/user/group, etc.)	"Policy"
8	Object path	AD path: *\local\amdom\ Users\testUser1*	AD path: *\local\amdom\ Users\testUser1*	*\zone\domain\GPO Display Name\Path*
9	The name of the server where Netwrix Auditor resides	-//-	-//-	-//-

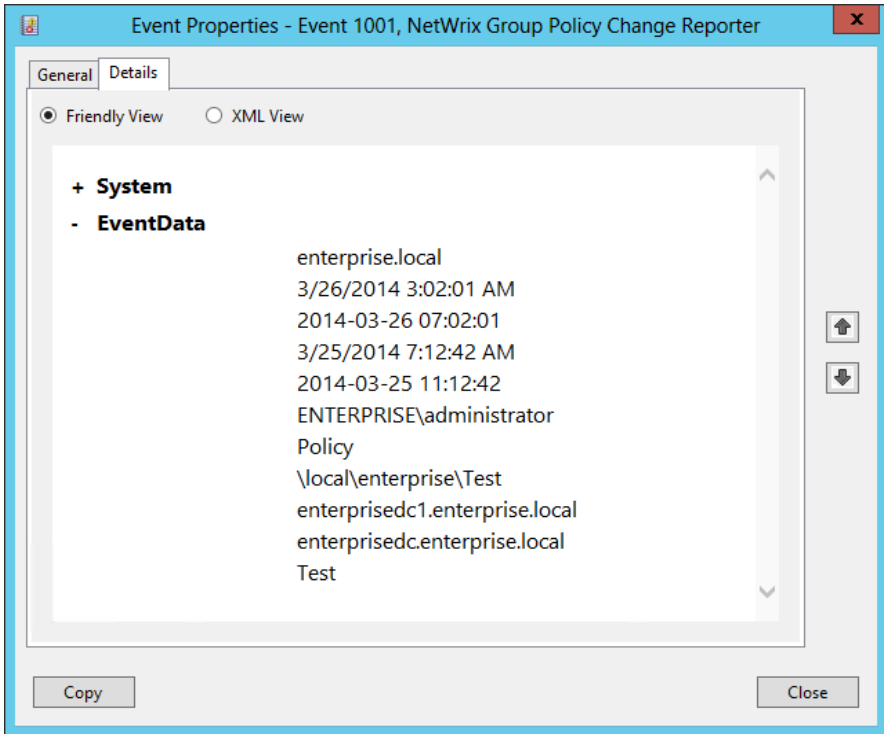
String number	Generic content	Active Directory Auditing	Exchange Server Auditing	Group Policy Auditing
10	The server where the change was made (DC, file server, etc.)	-//-	-//-	-//-
11	Custom field	Depends on type. The Active Directory Auditing-specific events have the following custom field values: • Distribution Domain Local Group • Distribution Global Group • Distribution Universal Group • Security Domain Local Group • Security Global Group • Universal Security Group	Schema-based name, e.g. msExchExchangeServer	GPO Display Name
12	Internal name of the attribute that was changed	-//-	-//-	GPO setting attribute name (currently is equivalent to [13], but should be changed to a real internal name when Group Policy Change Reporter provides this information)

String number	Generic content	Active Directory Auditing	Exchange Server Auditing	Group Policy Auditing
13	Display name of the attribute that was changed	-//-	-//-	Friendly attribute name (GPO setting attribute name)
14	The previous value of the attribute (or removed values if a multi-valued attribute). Can be empty.	-//-	-//-	-//-
15	The current value of the attribute (or added values if a multi-valued attribute). Can be empty.	-//-	-//-	-//-
16	Object GUID	AD object GUID	AD object GUID	Group Policy object GUID
17	Custom field	n/a	n/a	Group Policy Change Type: 1 - policy added 2 - policy removed 3- policy modified

NOTE:

- Local time is written in the default locale format (for example 03/16/2011 6:37:43 PM)
- UTC value is written the SQL date format (MM-DD-YYYY hh:mm:ss)

Review the event example:



8.5.2.2. General Events

The following table provides a description of the general events sorted by their ID.

ID	Name	Description
2001	Error	Error while processing Managed Object.
2002	Warning	Warning while processing Managed Object.
2010	Information	Audit data collection started.
2011	Information	Audit data collection completed successfully.
2012	Warning	Audit data collection completed with warnings.
2013	Error	Audit data collection completed with errors.

The following table describes the insertion strings displayed on the **Details** tab of the **Event Properties** dialog:

String number	Event ID	Description
1	All	Managed Object name (e.g. domain, computer collection, etc.)

String number	Event ID	Description
2	All	The name of the server where NetWrix software is installed
3	All	User account used for data collection
4	2001/2002	The error location (e.g. DC, server name, domain)
5	2001/2002	The error or warning message text

General events are recorded to the **Netwrix Change Reporter** event log to reflect the progress of a Managed Object processing. The following table explains the event recording sequence:

Step name	Generated events
Data collection start	Event 2010, one for each Managed Object.
Data processing	Events 2001 and 2002, if some errors or warnings occurred during data processing.
Data collection completed	One of the following events: 2011/2012/2013, representing the status of the data collection operation – e.g. *successful*, *with warnings* or *with errors*.

8.5.3. Event Samples

- Review the sample Audit events descriptions:
  - Review the sample Active Directory Auditing events descriptions
  - Review the sample Group Policy Auditing events descriptions
- Review the sample General events descriptions

Review the sample Active Directory Auditing events descriptions

Event ID: 1001

```
Who: system

What: \local\amdom\Configuration\Sites\Default-First-Site-
Name\Servers\MINV2\NTDS Settings\a8f9388b-89ff-41f7-83e8-cb1fdbd856bc

When: 03/17/2014 7:17:26 PM

Where: unknown

Change type: Added

Object type: nTDSConnection

Managed object: amdom.local
```

Detected by: amik.amdom.local at 03/17/2014 10:56:26 PM

Event ID: 1002

Who: system

What: \local\amdom\Users\state.local$

When: 03/17/2014 2:16:16 PM

Where: Agrig.amdom.local

Change type: Removed

Object type: user

Managed object: amdom.local

Detected by: amik.amdom.local at 03/17/2014 10:56:26 PM

Event ID: 1003

Who: EXCH2003B\Administrator

What: \LOCAL\EXC\EXCH2003\Users\Administrator

When: 03/17/2014 7:40:06 PM

Where: EXCH2003.EXCH2003.BYTSENKO.LOCAL

Change type: Modified

Object type: user

Change details: 'Storage Limits/Prohibit send at (Bytes)' changed from 'empty' to '124'

Managed object: exch2003.bytsenko.local

Detected by: amik.amdom.local at 03/17/2014 10:56:26 PM

Event ID: 1004

Who: AMDOM\Administrator

What: \local\amdom\amiks\TestUser4

When: 03/17/2014 7:17:06 PM

Where: Agrig.amdom.local

Change type: Modified

Object type: user

Managed object: amdom.local

Change details: User Account Disabled

Detected by: amik.amdom.local at 03/17/2014 10:56:26 PM

Event ID: 1005

Who: AMDOM\Admin

What: \local\amdom\OUAdmin

When: 03/17/2014 7:17:06 PM

Where: Agrig.amdom.local

Change type: Modified

Object type: organizationalUnit

Managed object: amdom.local

Change details: Object Security: Added: 'Permissions: Print Operators (Allow: Read permissions, Read all properties, List contents)'

Detected by: amik.amdom.local at 03/17/2014 10:56:26 PM

Event ID: 1006

Who: AMDOM\Administrator

What: \local\amdom\Users\test

When: 03/18/2014 7:17:06 PM

Where: Agrig.amdom.local

Change type: Modified

Object type: group

Managed object: amdom.local

Change details: Security Global Group Member: Removed: 'amdom.local/Users/newuser'

Detected by: amik.amdom.local at 03/18/2014 10:56:26 PM

Event ID: 1007

Who: system

What: \local\amdom\Configuration\Sites\Default-First-Site-Name\NTDS Site Settings

When: 03/17/2014 7:17:06 PM

Where: unknown

Change type: Modified

Object type: nTDSSiteSettings

Managed object: amdom.local

Change details: interSiteTopologyGenerator: modified and reverted back

Detected by: amik.amdom.local at 03/18/2014 6:56:26 AM

Review the sample Group Policy Auditing events descriptions

Event ID: 1001

```
The following audit event was detected:
Who: RABBIT\Administrator
What: \local\rabbit\New Group Policy Object
When: 06.04.2014 18:56:03
Where: DR-DC.rabbit.local
Change type: Added
Object type: Policy
Managed object: rabbit.local
Detected by: wks165.rabbit.local at 06.04.2014 18:57:52
```

Event ID: 1002

```
The following audit event was detected:
Who: RABBIT\Administrator
What: \local\rabbit\New Group Policy Object
When: 06.04.2014 19:00:49
Where: DR-DC.rabbit.local
Change type: Removed
Object type: Policy
Managed object: rabbit.local
Detected by: wks165.rabbit.local at 06.04.2014 19:02:24
```

Event ID: 1003

```
The following audit event was detected:
Who: RABBIT\Administrator
What: \local\rabbit\New Group Policy Object\General\Details
When: 06.04.2014 18:56:03
Where: DR-DC.rabbit.local
Change type: Modified
Object type: Policy
Change details: 'GPO Status' changed from '' to 'Enabled'
Managed object: rabbit.local
Detected by: wks165.rabbit.local at 06.04.2014 18:57:52
```

Review the sample General events descriptions

Event ID: 2001

```
The following warning has occurred on %Computer name% while processing %Object%: <warning text>
```

Event ID: 2002

```
The following error has occurred on %Computer name% while processing %Object%: <error text>
```

Event ID: 2010

```
Audit data collection for managed object %Object% started under user %User name%.
```

Event ID: 2011

```
Audit data collection for managed object %Object% completed successfully.
```

Event ID: 2012

```
Audit data collection for managed object %Object% completed with warnings. For details, see previous events.
```

Event ID: 2013

```
Audit data collection for managed object %Object% completed with errors. For details, see previous events.
```

8.5.4. SCOM Alerts

The SCOM alerts triggered by the Netwrix events can be divided into the following categories:

- Audit alerts—Are triggered by changes made to the Active Directory objects. These alerts help you detect unauthorized changes and violations of your security policy.
- Data Collection alerts—Are triggered by errors and warnings encountered during the data collection run by Netwrix Auditor.

Review the predefined SCOM alerts:

- Active Directory Auditing Alerts
- Group Policy Auditing Alerts
- Exchange Server Auditing Alerts

8.5.4.1. Active Directory Auditing Alerts

Alert name	Severity level	Trigger events	Rule description
		Audit alerts	
Administrative Group Membership Changed	Warning	Removing or adding members to the administration groups. The administration groups list includes: *Enterprise Admins, Domain Admins, Schema Admins, Account Operators, Administrators, Incoming Forest Trust Builders, Server Operators*, and *Backup Operators* groups.	Tracks changes to the administration groups membership.
Administrative Password Reset	Information	A user password has been reset.	Tracks changes to user password.
Changes to Domain Trust Relationships	Information	Any changes to domain trusts (for example, some trusts have been added or removed).	Tracks changes to domain trusts.
Domain Controller Modifications	Information	Any changes to properties of DC computer objects.	Tracks changes to Domain Controller computers.
Domain Controllers Demoted	Information	A domain controller has been demoted.	Monitors the demotion of domain controllers in the managed domains.
Domain Controllers Promoted	Information	A member server or a standalone computer has been promoted to domain controller.	Monitors the promotion of domain controllers in the managed domains.
Security Group Membership Changes	Information	Removing or adding members to security groups (including local, global, and universal groups).	Detects membership changes in all security groups.
Security Group Removed	Information	Deletion of security groups (including local, global, and universal groups).	Monitors deletions of security groups.
User Account Lockout	Warning	User account was locked.	Detects user account lockouts.

Alert name	Severity level	Trigger events	Rule description
User Account Disabled	Information	A user account was disabled.	Monitors disabling of users accounts.
Data collection alerts			
Data Collection Warning	Warning	The Active Directory Auditing feature within Netwrix Auditor encountered warnings while collecting data.	Monitors the status of Active Directory Auditing data collection tasks.
Data Collection Error	Critical	The Active Directory Auditing feature within Netwrix Auditor encountered warnings while collecting data.	Monitors the status of Active Directory Auditing data collection tasks.

8.5.4.2. Group Policy Auditing Alerts

Alert name	Severity level	Trigger events	Rule description
Audit alerts			
Account Lockout Policy Changes	Information	Any changes to the Account Lockout Policy settings.	Tracks changes to Account Lockout Policy Settings.
Audit Policy Changes	Information	Any changes to the Audit policy settings.	Tracks changes to the Audit policy settings.
Changes in GPO Links	Information	Any changes to GPO links.	Tracks changes to GPO links.
Default Domain Controllers Policy Changes	Critical	Any changes to the Default Domain Controllers GPO.	Tracks changes to the Default Domain Controllers GPO.
Interactive Logon Policy Changes	Information	Any changes to interactive logon rights.	Tracks changes to the Interactive Logon Policy.
Internet Explorer Policy Changes	Information	Any changes to Group Policy settings for Internet Explorer.	Tracks changes to Group Policy settings for Internet Explorer .

Alert name	Severity level	Trigger events	Rule description
Lockout Duration Policy Changes	Information	Any changes to the Account lockout duration Group Policy setting.	Tracks changes to the Account lockout duration Group Policy setting.
Logon and Logoff Script Policy Changes	Information	Any changes to Scripts (Logon/Logoff) Group Policy setting.	Tracks changes to Scripts (Logon/Logoff) Group Policy setting.
Network policy changes	Information	Any changes to the Network Group Policy setting.	Tracks changes to the Network Group Policy setting.
Password Age Policy Changes	Information	Any changes to the Password Age Group Policy setting.	Tracks changes to the Password Age Group Policy setting.
Password Complexity Policy Changes	Information	Any changes to the Password Complexity Group Policy setting.	Tracks changes to the Password Complexity Group Policy setting.
Password Encryption Policy Changes	Information	Any changes to the password Encryption Group Policy setting.	Tracks changes to the password Encryption Group Policy setting.
Password History Policy Changes	Information	Any changes to the Password History Group Policy setting.	Tracks changes to the Password History Group Policy setting.
Printer Policy Changes	Information	Any changes to the Printer Group Policy setting.	Tracks changes to the Printer Group Policy setting.
Public Key Policy Changes	Information	Any changes to the Public Key Group Policy setting.	Tracks changes to the Public Key Group Policy setting.
Registry Policy Changes	Information	Any changes to the Registry Group Policy setting.	Tracks changes to the Registry Group Policy setting.
Remote Installation Policy Changes	Information	Any changes to the Remote Installation Services setting.	Tracks changes to the Remote Installation Services setting.
Rename	Information	Any changes to the Accounts:	Tracks changes to the

Alert name	Severity level	Trigger events	Rule description
Administrator and Guest Policy Changes		rename administrator account and Accounts: Rename guest account Group Policy setting.	Accounts: rename administrator account and Accounts: Rename guest account Group Policy setting.
Restricted Groups Policy Changes	Information	Any changes to the Restricted Groups Policy setting.	Tracks changes to the Restricted Groups Policy setting.
Software Restriction Policy Changes	Information	Any changes to the Software Restriction Group Policy setting.	Tracks changes to the Software Restriction Group Policy setting.
Startup and Shutdown Script Policy Changes	Information	Any changes to the Scripts (Startup/Shutdown) Group Policy settings.	Tracks changes to the Scripts (Startup/Shutdown) Group Policy settings.
System Policy Changes	Information	Any changes to the System Policy setting.	Tracks changes to the System Policy setting.
System Services Policy Changes	Information	Any changes to the System Services Policy setting.	Tracks changes to the System Services Policy setting.
User Rights Assignment Policy Changes	Information	Any changes to the User Rights Assignment Group Policy Setting.	Tracks changes to the User Rights Assignment Group Policy Setting.
Windows Components Policy Changes	Information	Any changes to the Windows Components Group Policy setting.	Tracks changes to the Windows Components Group Policy setting.
Wireless Network Policy Changes	Information	Any changes to the Wireless Network Policy setting.	Tracks changes to the Wireless Network Policy setting.
Data collection alerts			
Data Collection Warning	Warning	The Group Policy Auditing feature within Netwrix Auditor encountered warnings while collecting data.	Monitors the status of Group Policy Auditing data collection tasks.

Alert name	Severity level	Trigger events	Rule description
Data Collection Error	Critical	The Group Policy Auditing feature within Netwrix Auditor encountered warnings while collecting data.	Monitors the status of Group Policy Auditing data collection tasks.

8.5.4.3. Exchange Server Auditing Alerts

Alert name	Severity level	Trigger events	Rule description
Audit alerts			
Address List Added	Information	Adding new Exchange address list.	Detects adding of new Exchange address list.
Address List Changed	Information	Adding or removing recipients from Exchange address list, or any changes to its properties.	Detects changes to Exchange address lists.
Address List Removed	Information	Removing Exchange address list.	Detects removing of Exchange address lists.
Mailbox Delegation	Warning	Any changes to mailbox delegation permissions.	Tracks changes to mailbox permissions.
Mailbox Quota Changed	Warning	Mailbox quota change.	Detects any changes to mailbox quota.
Mailbox Security Changed	Warning	Any changes to mailbox security permissions.	Detects changes to mailbox security permissions.
Mailbox Settings Changed	Information	Any changes to mailbox settings.	Detects any changes to mailbox settings.
MS Exchange Storage Group Added	Information	Creation of new Exchange Storage group.	Tracks creations of new Exchange Storage groups.
MS Exchange Storage Group Removed	Information	Deletion of existing Exchange Storage groups.	Tracks deletions of Exchange Storage groups.

Alert name	Severity level	Trigger events	Rule description
MS Exchange Storage Group Changed	Information	Any changes to Exchange Storage groups.	Tracks changes to Exchange Storage groups.
MS Exchange Store Added	Information	Creation of new Exchange store.	Tracks creations of new Exchange stores.
MS Exchange Store Removed	Information	Deletions of existing Exchange stores.	Tracks changes to Exchange stores.
MS Exchange Server Added	Information	Installation of new Exchange Server in your environment.	Monitors addition of new Exchange Servers to your environment.
Recipient Policy Added	Information	Adding new recipient policies.	Detects newly created recipient policies.
Recipient Policy Changed	Information	Any changes to recipient policy (for example, changes to mailbox storage limits).	Tracks changes made to recipient policy settings and permissions.
Recipient Policy Removed	Information	Removing recipient policies.	Detects deletion of existing recipient policies.
Recipient Update Services Added	Information	Adding new Exchange Recipient Update Service to your organization.	Monitors addition of new Exchange Recipient Update Services to your environment.
Recipient Update Services Removed	Information	Removing Exchange Recipient Update Service from your organization.	Monitors deletion of Exchange Recipient Update Services.
Recipient Update Services Changed	Information	Any changes to the Exchange Recipient Update Service.	Monitors changes made to Exchange Recipient Update Services.

Data collection alerts

Alert name	Severity level	Trigger events	Rule description
Data Collection Warning	Warning	The Exchange Server Auditing feature within Netwrix Auditor encountered warnings while collecting data.	Monitors the status of Exchange Server Auditing data collection tasks.
Data Collection Error	Critical	The Exchange Server Auditing feature within Netwrix Auditor encountered warnings while collecting data.	Monitors the status of Exchange Server Auditing data collection tasks.

9. Appendix

9.1. Monitored Object Types and Components

Review the list of object types, attributes and components monitored and reported by Netwrix Auditor.

- Object Types and Attributes Monitored by Active Directory Auditing
- Object Types and Attributes Monitored by Windows File Server Auditing
- Components and Settings Monitored by Windows Server Auditing
- Object Types and Attributes Monitored by VMware Auditing
- Object and Data Types Monitored by SQL Server Auditing
- Object Types and Attributes Monitored by SharePoint Auditing

9.1.1. Object Types and Attributes Monitored by Active Directory Auditing

The Active Directory Auditing feature within Netwrix Auditor tracks changes made to all object classes and attributes in the Active Directory Domain, Configuration and Schema partitions. It also tracks changes to new object classes and attributes added due to the Active Directory Schema extension. For detailed information, refer to Microsoft articles:

- A full list of Active Directory object classes
- A full list of Active Directory object attributes

9.1.2. Components and Settings Monitored by Windows Server Auditing

Review a full list of all components and settings monitored by the Windows Server Auditing feature.

- General Computer Settings
- Add / Remove Programs
- Services
- Hardware
- Scheduled Tasks
- Local Users and Groups
- DNS Configuration*

- DNS Resource Records*
- Windows Registry Settings

NOTE: The **Who Changed** value is reported as *"Not Applicable"* for the components and settings marked with asterisk (*).

Object Type	Attributes
	General Computer Settings
Computer Name	• Computer Description • Name • Domain
Environment Variables	• Type • Value
General	• Caption • Organization • Registered User • Serial Number • Service Pack* • Version*
Remote	• Enable Remote Desktop on this computer
Startup and Recovery	• Automatically Restart • Dump File • Dump Type • Overwrite any existing file • Send Alert • Small Dump Directory • System Startup Delay • Write an Event
System Restore	• State **NOTE:** This attribute is only reported for computers running Windows XP/2003

Object Type	Attributes
	Add / Remove Programs
Add or Remove Programs	• Installed For* • Version
	Services
System Service	• Action in case of failed service startup • Allow service to interact with desktop • Caption • Description Name • Path to executable • Service Account • Service Type • Start Mode
	Hardware
Base Board*	• Hosting Board • Status • Manufacturer • Product • Version • Serial Number
BIOS*	• Manufacturer • Version
Bus*	• Bus Type • Status
Cache Memory*	• Configuration Manager Error Code • Last Error Description • Last Error Code

Object Type	Attributes
	• Purpose • Status
CD-ROM Drive*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Media Type • Name • SCSI Bus • SCSI Logical Unit • SCSI Port • SCSI Target ID • Status
Disk Partition*	• Primary Partition • Size (bytes) • Starting offset (bytes)
Display Adapter*	• Adapter RAM (bytes) • Adapter Type • Bits/Pixel • Configuration Manager Error Code • Driver Version • Installed Drivers • Last Error Description • Last Error Code • Refresh Rate • Resolution • Status
DMA*	• Status

Object Type	Attributes
Floppy Drive*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
Hard Drive*	• Bytes/Sector • Configuration Manager Error Code • Interface Type • Last Error Description • Last Error Code • Media Loaded • Media Type • Model • Partitions • SCSI Bus • SCSI Logical Unit • SCSI Port • SCSI Target ID • Sectors/Track • Size (bytes) • Status • Total Cylinders • Total Heads • Total Sectors • Total Tracks • Tracks/Cylinder
IDE*	• Configuration Manager Error Code • Description • Last Error Description

Object Type	Attributes
	• Last Error Code • Status
Infrared*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
Keyboard*	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code • Layout • Name • Status
Logical Disk*	• Description • File System • Size (bytes) • Status
Monitor*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Monitor Type • Status
Network Adapter	• Adapter Type • Configuration Manager Error Code • Default IP Gateway • DHCP Enabled • DHCP Server

Object Type	Attributes
	• DNS Server Search Order • IP Address • Last Error Description • Last Error Code • MAC Address • Network Connection Name • Network Connection Status • Service Name • Status
Network Protocol*	• Description • Status
Parallel Ports*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
PCMCIA Controller*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
Physical Memory*	• Capacity (bytes) • Status • Manufacturer • Memory Type • Speed • Part Number • Serial Number
Pointing Device*	• Configuration Manager Error Code

Object Type	Attributes
	• Double Click Threshold • Handedness • Hardware Type • Last Error Description • Last Error Code • Number of buttons • Status
Printing	• Comment* • Hidden* • Local* • Location* • Name* • Network* • Port Name* • Printer error information • Published* • Shared* • Share Name* • Status
Processor*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Max Clock Speed (MHz) • Name • Status
SCSI*	• Configuration Manager Error Code • Description • Last Error Description

Object Type	Attributes
	• Last Error Code • Status
Serial Ports*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Maximum Bits/Second • Name • Status
Sound Device*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
System Driver	• Description • Error Control • Start Mode • Service Type
System Slot*	• Slot Designation • Status
USB Controller*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Name • Status
USB Hub*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Name

Object Type	Attributes
	• Status
	Scheduled Tasks
Scheduled Task	• Account Name • Application • Comment • Creator • Enabled • Parameters • Triggers
	Local Users and Groups
Local Group	• Description • Name • Members
Local User	• Description • Disabled/Enabled • Full Name • Name • User cannot change password • Password Never Expires • User must change password at next logon
	DNS Configuration*
DNS Server	• Address Answer Limit • Allow Update • Auto Cache Update • Auto Config File Zones • Bind Secondaries • Boot Method

Object Type	Attributes
	• Default Aging State • Default No Refresh Interval • Default Refresh Interval • Disable Auto Reverse Zones • Disjoint Nets • Ds Available • Ds Polling Interval • Ds Tombstone Interval • EDns Cache Timeout • Enable Directory Partitions • Enable Dns Sec • Enable EDns Probes • Event Log Level • Forward Delegations • Forwarders • Forwarding Timeout • Is Slave • Listen Addresses • Local Net Priority • Log File Max Size • Log File Path • Log IP Filter List • Log Level • Loose Wildcarding • Max Cache TTL • Max Negative Cache TTL • Name Check Flag • No Recursion • Recursion Retry

Object Type	Attributes
	• Recursion Timeout • Round Robin • Rpc Protocol • Scavenging Interval • Secure Responses • Send Port • Server Addresses • Strict File Parsing
DNS Zone	• Aging State • Allow update • Auto created • Availability for scavenge time • Data file name • Ds integrated • Expires after • Forwarder slave • Forwarder timeout • Last successful soa check • Last successful Xfr • Master servers • Minimum TTL • No refresh interval • Notify • Notify servers • Owner name • Paused • Primary server • Refresh interval

Object Type	Attributes
	• Refresh interval • Responsible person • Retry interval • Reverse • Scavenge servers • Secondary servers • Secure secondaries • Shutdown • TTL • Use wins • Zone type
DNS Domain	• Container Name
	DNS Resource Records*
DNS AAAA	• Container name • IPv6 Address • Owner name • TTL
DNS AFSDB	• Container name • Owner name • Server name • Server subtype • TTL
DNS ATM A	• ATM Address • Container name • Format • Owner name • TTL

Object Type	Attributes
	• Value
DNS A	• Container name • IP Address • Owner name • TTL
DNS CNAME	• Container name • FQDN for target host • Owner name • TTL
DNS DHCID	• Container name • DHCID (base 64) • Owner name • TTL
DNS DNAME	• Container name • FQDN for target domain • Owner name • TTL
DNS DNSKEY	• Algorithm • Container name • Key type • Key (base 64) • Name type • Owner name • Protocol • Signatory field • TTL
DNS DS	• Key tag

Object Type	Attributes
DNS HINFO	• Container name • CPU type • Operating system • Owner name • TTL
DNS ISDN	• Container name • ISDN phone number and DDI • ISDN subaddress • Owner name • TTL
DNS KEY	• Algorithm • Container name • Key type • Key (base 64) • Name type • Owner name • Protocol • Signatory field • TTL
DNS LOC	• Container name • MF host • Owner name • TTL
DNS MB	• Container name • Mailbox host • Owner name • TTL

Object Type	Attributes
DNS MD	• Container name • MD host • Owner name • TTL
DNS MF	• Container name • MF host • Owner name • TTL
DNS MG	• Container name • Member mailbox • Owner name • TTL
DNS MINFO	• Container name • Error mailbox • Owner name • Responsible mailbox • TTL
DNS MR	• Container name • Owner name • Replacement mailbox • TTL
DNS MX	• Container name • FQDN of mail server • Mail server priority • Owner name • TTL
DNS NAPTR	• Container name

Object Type	Attributes
	• Flag string • Order • Owner name • Preference • Regular expression string • Replacement domain • Service string • TTL
DNS NS	• Container name • Name servers • Owner name • TTL
DNS NXT	• Container name • Next domain name • Owner name • Record types • TTL
DNS PTR	• Container name • Owner name • PTR domain name • TTL
DNS Resource Record	• Owner name • Record class • TTL • Zone type
DNS RP	• Container name • Mailbox of responsible person

Object Type	Attributes
	• Optional associated text (TXT) record • Owner name • TTL
DNS RRSIG	• Algorithm • Container name • Key tag • Labels • Original TTL • Owner name • Signature expiration (GMT) • Signature inception (GMT) • Signature (base 64) • Signer's name • TTL • Type covered
DNS RT	• Container name • Intermediate host • Owner name • Preference • TTL
DNS SIG	• Algorithm • Container name • Key tag • Labels • Original TTL • Owner name • Signature expiration (GMT) • Signature inception (GMT)

Object Type	Attributes
	• Signature (base 64) • Signer's name • TTL • Type covered
DNS SRV	• Container name • Host offering this service • Owner name • Port number • Priority • TTL • Weight
DNS TEXT	• Container name • Owner name • Text • TTL
DNS WINS	• Cache time-out • Container name • Do not replicate this record • Lookup time-out • Owner name • Wins servers
DNS WINSR	• Cache time-out • Container name • Domain to append to returned name • Do not replicate this record • Lookup time-out • Owner name • Submit DNS domain as NETBIOS scope

Object Type	Attributes
DNS WKS	• Container name • IP address • Owner name • Protocol • Services • TTL
DNS X25	• Container name • Owner name • Record • TTL • X.121 PSDN address
	Windows Registry Settings
OS Security	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\FileSystem(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\NetworkProvider (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\Print\\Providers\\LanMan Print Services(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\SecurePipeServers (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\Environment(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\SubSystems(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\Memory Management(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\Executive(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\KnownDLLs(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\Windows(|\\.*)

Object Type	Attributes
	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Image File ExecutionOptions(|\\.*)
Security Settings	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\DrWatson(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Driver Signing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Non-Driver Signing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\MSDTC(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\NetDDE(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows\\CurrentVersion\\Policies\\System(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Explorer\\BitBucket(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Group Policy(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Installer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Policies\\System(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\policies\\Network(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\policies\\Ratings(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\policies\\system(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\AEDebug(|\\.*)

Object Type	Attributes
	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\AsrCommands(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Perflib(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\SeCEdit(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Setup\\RecoveryConsole(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\PCHealth\\ErrorReporting(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Conferencing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\EventViewer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Messenger\\Client(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\SearchCompanion(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\SystemCertificates\\AuthRoot(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\W32time\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\DCOM(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\IIS(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\Printers(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\Rpc(|\\.*)

Object Type	Attributes
	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\DriverSearching(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Group Policy(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Installer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Internet Connection Wizard(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Network Connections(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Registration Wizard Control(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Peernet(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\WindowsFirewall\\ StandardProfile\\IcmpSettings(|\\.*) • HKEY_LOCAL_MACHINE\\System\\Clone(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\Control\\SessionManager(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\WinLogon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\CrashControl (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\FileSystem(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\LSA(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\Print\\Providers\\LanManPrint Services\\Servers(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\ProductOptions (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SecurePipeServers\\WinReg(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\kernel(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\WMI\\Security

Object Type	Attributes
	(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Enum(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Hardware Profiles(|\\.*) • HKEY_USERS\\.DEFAULT\\Software\\ Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_USERS\\.Default\\Software\\Microsoft\\NetDDE(|\\.*) • HKEY_USERS\\.Default\\Software\\Microsoft\\ SystemCertificates\\Root\\ProtectedRoots(|\\.*)
Patches	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Hotfix(|\\.*)
Windows Firewall	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\WindowsFirewall\\DomainProfile(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\WindowsFirewall\\StandardProfile(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\cryptography(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\windows\\safer\\codeidentifiers(|\\.*)
Remote Desktop	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\Terminal Server\\WinStations\\RDP-Tcp(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\ Policies\\Microsoft\\Windows NT\\Terminal Services(|\\.*)
File Sharing Settings	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Services\\LanmanServer\\Shares(|\\.*)
USB Devices	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\USBSTOR(|\\.*)
Important Services	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Schedule(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WebClient(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WmiApSrv(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\upnphost(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AFD(|\\.*)

Object Type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Alerter(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AppMgmt(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AppMgr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Appmon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\BINLSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\ \Services\\Browser(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Cdrom(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\CiSvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Clipsrv(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Services\\Eventlog\\Application(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Eventlog\\Security (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Eventlog\\System (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Fax(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\HTTPFilter(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\IISADMIN(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\IPSEC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Services\\LanManServer\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Services\\LanmanWorkstation\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\LicenseService (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MSDTC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MSFtpsvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MacFile(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MacPrint(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Messenger(|\\.*)

Object Type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MrxSmb(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NTDS(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\NWCWorkstation (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NetBT(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Netlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Netman(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NntpSvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NtFrs(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\POP3Svc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RDSessMgr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RasAuto(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RasMan(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RemoteAccess (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RemoteRegistry (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Remote_Storage_ Server(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Remote_Storage_ User_Link(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RpcLocator(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SMTPSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SNMPTRAP(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SNMP(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SharedAccess (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Spooler(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SrvcSurg(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TapiSrv(|\\.*)

Object Type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Tcpip(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TermService(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TlntSvr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\W3SVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WZCSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\helpsvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\ldap(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\mnmsrvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\tftpd(|\\.*)
Startup and autorun	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\IniFileMapping(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows\\CurrentVersion\\Run(|\\.*)
All other settings	• All keys from HKLM\Software, HKLM\System, HKU\Default that are not covered by the masks of other categories

9.1.3. Object Types and Attributes Monitored by Windows File Server Auditing

Review a full list of object types monitored by the Windows File Server Auditing feature.

NOTE: The attributes marked with asterisk (*) cannot be monitored if the **Large server support** option is enabled.

Object Type	Attributes
File	• Attributes • Security • Size • Date Created • Date Modified
Folder	• Security

Object Type	Attributes
	• Attributes • Date Created • Date Modified
Share	• Share Permissions* • User Limit* • Local Path* • Root Folder Security • Attributes* • Date Created • Date Modified

9.1.4. Object and Data Types Monitored by SQL Server Auditing

Review a full list of all object and data types monitored by the SQL Server Auditing feature.

- Monitored Object Types
- Monitored Data Types

9.1.4.1. Monitored Object Types

NOTE: The attributes marked with asterisk (*) cannot be monitored on SQL Server 2000.

Object Type	Attributes
Application Role	• Date Created • Date Modified • Default Schema • Extended Properties • Id • Name • Owned Schemas

Object Type	Attributes
Backup	• Backup name • Description • Device name • logical_device_name • Size • Type
Column	• Allow nulls • ANSI Padding Status • Collation • Computed Text • Default Constraint • Full Text • ID • Identity • Identity increment • Identity seed • Is Computed • Length • Name • Not for replication • Numeric precision • Numeric scale • Primary Key • Rule • Rule Schema • System Type • XML Schema Namespace
Constraints	• Date Created

Object Type	Attributes
	• Date Modified • Definition • ID • Is system named • MS shipped • Name • Published • Schema published
Credential	• Id • Identity • Date Created • Date Modified • Name
Database	• Compatibility • Database Size • Database Space Available • Date Created • Date Modified • Extended Properties • File Id • File Group • File Name • Growth • Id • Name • Options • Owner • Permissions

Object Type	Attributes
	• Size • Usage
Database role	• Date Created • Date Modified • Extended Properties • Id • Name • Owner • Owned Schemas • Role Members
Functions	• Date Created • Date Modified • Id • Name • Permissions • Type
Login	• Date Created • Date Modified • Default Database • Default Language • Disabled • Enforce Password Expiration • Enforce Password Policy • Id • Name • Password Hash • Server Roles

Object Type	Attributes
Restore	• Type
Schema	• Date Created • Date Modified • Extended Properties • Id • Name • Owner • Permissions
Server instance	• Ad Hoc Distributed Queries* • Affinity I/O Mask • Affinity Mask • Agent XPs* • Allow Updates • Awe Enabled • Blocked Process Threshold* • C2 Audit Mode • Clr Enabled* • Collation • Cost Threshold For Parallelism • Cross Db Ownership Chaining* • Cursor Threshold • Database Mail XPs* • Date Modified • Default Full-text Language • Default Language • Default Trace Enabled* • Disallow Results From Triggers • Fill Factor (%)

Object Type	Attributes
	• Ft Crawl Bandwidth (max)* • Ft Crawl Bandwidth (min)* • Ft Notify Bandwidth (max)* • Ft Notify Bandwidth (min)* • Id • In-doubt Xact Resolution* • Index Create Memory (K) • Lightweight Pooling • Locks • Max Degree Of Parallelism • Max Full-text Crawl Range* • Max Server Memory (M) • Max Text Repl Size (B) • Max Worker Threads • Media Retention • Min Memory Per Query (K) • Min Server Memory (M) • Name • Nested Triggers* • Network Packet Size (B) • Ole Automation Procedures* • Open Objects • Permissions • PH Timeout (s)* • Precompute Rank* • Priority Boost • Query Wait (s) • Query Governor Cost Limit • Recovery Interval (min)

Object Type	Attributes
	• Remote Admin Connections* • Remote Login Timeout (s) • Remote Proc Trans • Remote Query Timeout (s) • Remote Access • Replication XPs* • Scan For Startup Procs • Server Trigger Recursion* • Set Working Set Size • Show Advanced Options • SMO And DMO XPs* • SQL Mail XPs* • Status • Transform Noise Words* • Two Digit Year Cutoff • User Connections • User Instances Enabled* • User Instance Timeout* • User Options • Web Assistant Procedures* • Xp_cmdshell*
Server role	• Date Created • Date Modified • Id • Name • Role Members
SQL job	• Automatically delete job • Category

Object Type	Attributes
	• Date Created • Date Modified • Description • Email notification • Email operator • Enabled • ID • Name • Net send notification • Net send operator • Owner • Page notification • Page operator • Schedules • Write to the Windows Application event log
SQL job schedule	• ID • Name • On Failure • On Success • Output file • Process exit code of a successful command • Retry attempts • Retry interval (minutes) • Step • Type
SQL job schedule	• Date Created • Date Modified • Enabled

Object Type	Attributes
	• ID • Name • Owner • Schedule Type • Settings
Stored procedure	• ANSI NULLs • Date Created • Date Modified • Encrypted • Execute us • FOR replication • Id • Name • Permissions • Quoted Identifier • Recompile • Schema
Table	• ANSI NULLs • Date Created • Date Modified • Filegroup • Id • Name • Partition scheme • Permissions • Schema • Table is partitioned • Table is replicated

Object Type	Attributes
	• Text filegroup
Table keys	• Name • ID • Date Created • Date Modified • MS shipped • Published • Schema published • Disabled • Not for replication • Not trusted • Delete referential action • Update referential action • Is system named
Triggers	• Date Created • Date Modified • Disabled • ID • Instead of trigger • MS shipped • Name • Not for replication
User	• Date Created • Date Modified • Default Schema • Extended Properties • Id • Name

Object Type	Attributes
	• Owned Schemas • Roles
View	• ANSI NULLs • Date Created • Date Modified • Encrypted • Id • Name • Permissions • Quoted Identifier • Schema • Schema bound
View column	• Allow nulls • ANSI Padding Status • Collation • Computed Text • Default Constraint • Full Text • ID • Identity • Identity increment • Identity seed • Is Computed • Length • Name • Not for replication • Numeric precision • Numeric scale

Object Type	Attributes
	• Rule • Rule Schema • System Type • XML Schema Namespace • XML Schema Namespace schema
View index	• Allow Page Locks • Allow Row Locks • ID • Data Space ID • Disabled • Fill Factor • Hypothetical • Ignore Dup Key • Name • Padindex • Primary Key • Schema Name • Type • Unique • Unique Constraint • View Name
View index column	• Column ID • ID • Included Column • Index ID • Key Ordinal • Name • Partition Ordinal

Object Type	Attributes
	• Schema Name • Sort Order • View Name

9.1.4.2. Monitored Data Types

The following list contains the names of all data types monitored by SQL Server Auditing.

bigint	hierarchyid	smallint
bit	int	smallmoney
char	float	table
cursor	money	time
date	nchar	timestamp
datetime2	nvarchar	tinyint
datetime	numeric	uniqueidentifier
datetimeoffset	real	varchar
decimal	smalldatetime	xml

9.1.5. Object Types and Attributes Monitored by VMware Auditing

Review a full list of object types and attributes monitored by VMware Auditing.

Object type	Attribute
Virtual Machine	• Snapshot Name • Snapshot Description • Current Snapshot • Power State • Guest State • Virtual Machine Name • Guest OS • Guest OS Version

Object type	Attribute
	• Memory Size (M) • Power Off Type • Suspend Type • Run VMware Tools Scripts After Powering On • Run VMware Tools Scripts After Resuming • Run VMware Tools Scripts Before Powering Off • Run VMware Tools Scripts Before Suspending • Guest Power Management • Disable Acceleration • Enable Logging • Record Debugging Information • Synchronize guest time with host • Check and upgrade Tools • Hyper-threaded Core Sharing • Swap file Location • Hardware Page Table Virtualization • Force BIOS Setup • Power-on Boot Delay • Power On • Advanced Configuration • Number of virtual processors • Operation mode of guest OS • Notes • Annotation • ResourcePool • Template • Connected • Connect at power on • VirtualCdrom Device Type

Object type	Attribute
	• VirtualCdrom Mode • VirtualParallelPort Port • VirtualParallelPort Connection • VirtualSerialPort Connection • VirtualSerialPort Yield CPU on poll • VirtualSerialPort Near End • VirtualSerialPort Far End • VirtualPCNet32 MAC Address Type • VirtualPCNet32 MAC Address • VirtualPCNet32 Wake on LAN • VirtualPCNet32 IP Address • VirtualPCNet32 Network Adapter Name • VirtualPCNet32 Network Adapter Network • VirtualPCNet32 Network Adapter MAC • VirtualFloppy Device Type • VirtualSCSIController Controller Type • VirtualSCSIController Bus Sharing • VirtualSCSIController Bus Number • VirtualDisr Disk Mode • VirtualDisr Unit Number • VirtualDisr Capacity(K) • VirtualDisr Share Level • VirtualDisr Datastore
Alarm	• Name • Description • Yellow Zone Value • Red Zone Value • Enable

Object type	Attribute
Authorization Manager	• Privilege • Authorization Manager Name
Cluster Resource	• Name • VMware HA • VMware DRS • VMware HA Admission Control • VMware HA Isolation Response • VMware HA Restart Priority • VMware HA Number of host failures allowed • VMware HA Advanced Option • VMware DRS Automation Level • VMware DRS Migration threshold • Swap Policy for Virtual Machines • VMware HA Isolation Response • VMware HA Restart Priority • VMware DRS Power Management • VMware DRS 'Keep Virtual Machines Together' Rule Name • VMware DRS 'Keep Virtual Machines Together' Rule Enabled • VMware DRS 'Keep Virtual Machines Together' Rule Status • VMware DRS 'Keep Virtual Machines Together' Rule Virtual Machine • VMware DRS 'Separate Virtual Machines' Rule Name • VMware DRS 'Separate Virtual Machines' Rule Enabled • VMware DRS 'Separate Virtual Machines' Rule Status • VMware DRS 'Separate Virtual Machines' Rule Virtual Machine • VMware DRS Virtual Machine Automation Mode • Available CPU • Available Memory • Available Hosts

Object type	Attribute
Computer Resource	• Name
Datacenter	• Name
Data Store	• Accessible • Name
Folder	• Folder Name
Host System	• Overall Status • Configuration Status • CPU Expandable Reservation • CPU Limit • CPU Reservation • CPU Shares Level • CPU Shares • Memory Expandable Reservation • Memory Limit • Memory Reservation • Memory Shares Level • Memory Shares • Datastore accessible to Host • NTP required • NTP uninstallable • NTP running • NTP policy • NTP Servers • Port Group Allow Promiscuous • Port Group MAC Address Changes • Port Group Forged Transmits • Port Group VLAN ID

Object type	Attribute
	• Port Group Attached uplink adapter • Virtual Switch Allow Promiscuous • Virtual Switch MAC Address Changes • Virtual Switch Forged Transmits • Virtual Switch Number of Ports • Virtual Switch Attached uplink adapter • VMkernel IP Address of port • Service Console IP Address of port
Resource Pool	• Name

9.1.6. Object Types and Attributes Monitored by SharePoint Auditing

Review a full list of object types and attributes monitored by SharePoint Auditing.

NOTE: The attributes marked with asterisk (*) are reported without details, only the fact of change is reported.

Object type	Attribute
Group	• Membership
Permission Level	• Permissions
Site	• Site URL • Permissions • Permission Inheritance
List	• Permissions • Permission Inheritance
List Item	• Attachments • Permissions

Object type	Attribute
	• Permission Inheritance • List Item Properties*
Document	• Document URL • Permissions • Permission Inheritance • Document Properties* • Content Modifications*
Farm	• Configuration Database • Configuration Database Server • Version • Managed Account for "Web Application Pool - {name}" • Managed Account for "Service Application Pool - {name}" • Managed Account for "Windows Service - {name}" • Managed Account for "Farm Account" • Managed Accounts
Web Application	• Web Application URL • Name • Port • User Permissions • Alternate Access Mappings • Content Database • Blocked File Extensions
Site Collection	• Site Collection URL • Content Database • Content Database Server • Site Storage Maximum Limit • Site Storage Warning Limit • Sandboxed Solutions Resource Maximum Quota

Object type	Attribute
	• Sandboxed Solutions Resource Warning Quota • Quota Template • Lock Status
Server	• Name
Service	• Name • Status
Permission Policy Level	• Name • Grant Permissions • Deny Permissions • Site Collection Permissions
User Policy	• Display Name • Permissions
Anonymous Policy	• Zone • Permissions
Farm Solution	• Name • Status • Last Operation Time
Farm Feature	• Name • Status

9.2. Install ADSI Edit

The ADSI Edit utility is used to view and manage objects and attributes in an Active Directory forest. ADSI Edit is required to manually configure audit settings in the target domain. It must be installed on any domain controller in the domain you want to start auditing.

To install ADSI Edit on Windows 7

1. Download and install Remote Server Administration Tools that include ADSI Edit.
2. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or**

off.

3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **Install**.

To install ADSI Edit on Windows Server 2008 and Windows Server 2008 R2

1. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Features** in the left pane, click **Add Features**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **Install** to enable it.

To install ADSI Edit on Windows Server 2012

1. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Features** in the left pane.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **Next** to proceed to confirmation page.
5. Click **Install** to enable it.

To install ADSI Edit on Windows 8

1. Download and install Remote Server Administrator Tools that include Group Policy Management Console.
2. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.

9.3. Install Microsoft SQL Server

This section provides instructions on how to:

- Install Microsoft SQL Server 2008 R2 Express or 2012 Express
- Verify Reporting Services Installation

9.3.1. Install Microsoft SQL Server 2008 R2 Express or 2012 Express

NOTE: This section only provides instructions on how to install SQL Server with Advanced Services and configure the Reporting Services required for Netwrix Auditor to function properly. For full installation and configuration instructions, refer to Microsoft documentation.

1. Download one of the following:
   - SQL Server 2008 R2
   - SQL Server 2012
2. Run the installation package and follow the instructions of the wizard until you get to the **Feature Selection** page. On this page, ensure that the **Reporting Services** option is selected under **Instance Features**.
3. Proceed with the wizard until you get to the **Server Configuration** page. On this page, ensure that the **SQL Server Reporting Services** will run under the **Network Service account**, and its startup type is set to *"Automatic"*.
4. Follow the instructions of the wizard to complete the installation.

9.3.2. Verify Reporting Services Installation

As a rule, Netwrix Auditor can use Reporting Services installed with the default settings. However, to ensure that Reporting Services are properly configured, it is recommended to perform the following procedure:

NOTE: You must be logged in as a member of the local administrators group on the computer where SQL Server 2008 R2 or 2012 Express is installed.

1. Depending on SQL Server version installed, navigate to:
   - **Start** → **All Programs** → **Microsoft SQL Server 2008 R2** → **Configuration Tools** → **Reporting Services Configuration Manager**
   - **Start** → **All Programs** → **Microsoft SQL Server 2012** → **Configuration Tools** → **Reporting Services Configuration Manager**
2. In the **Reporting Services Configuration Connection** dialog, make sure that your local report server instance (for example SQLExpress) is selected and click **Connect**.
3. In the **Reporting Services Configuration Manager** left pane, select **Web Service URL**. Make sure that **Virtual Directory** is set to *"ReportServer_<YourSqlServerInstanceName>"* (for example ReportServer_SQLEXPRESS for SQLEXPRESS instance) and **TCP Port** is set to *"80"*.
4. In the **Reporting Services Configuration Manager** left pane, select **Database**. Make sure that the **SQL Server Name** and **Database Name** fields contain correct values. If not, click **Change Database**

and complete the **Report Server Database Configuration** wizard.

5. In the **Reporting Services Configuration Manager** left pane, select **Report Manager URL**. Make sure **Virtual Directory** is set correctly, and that the URL is valid.

Index