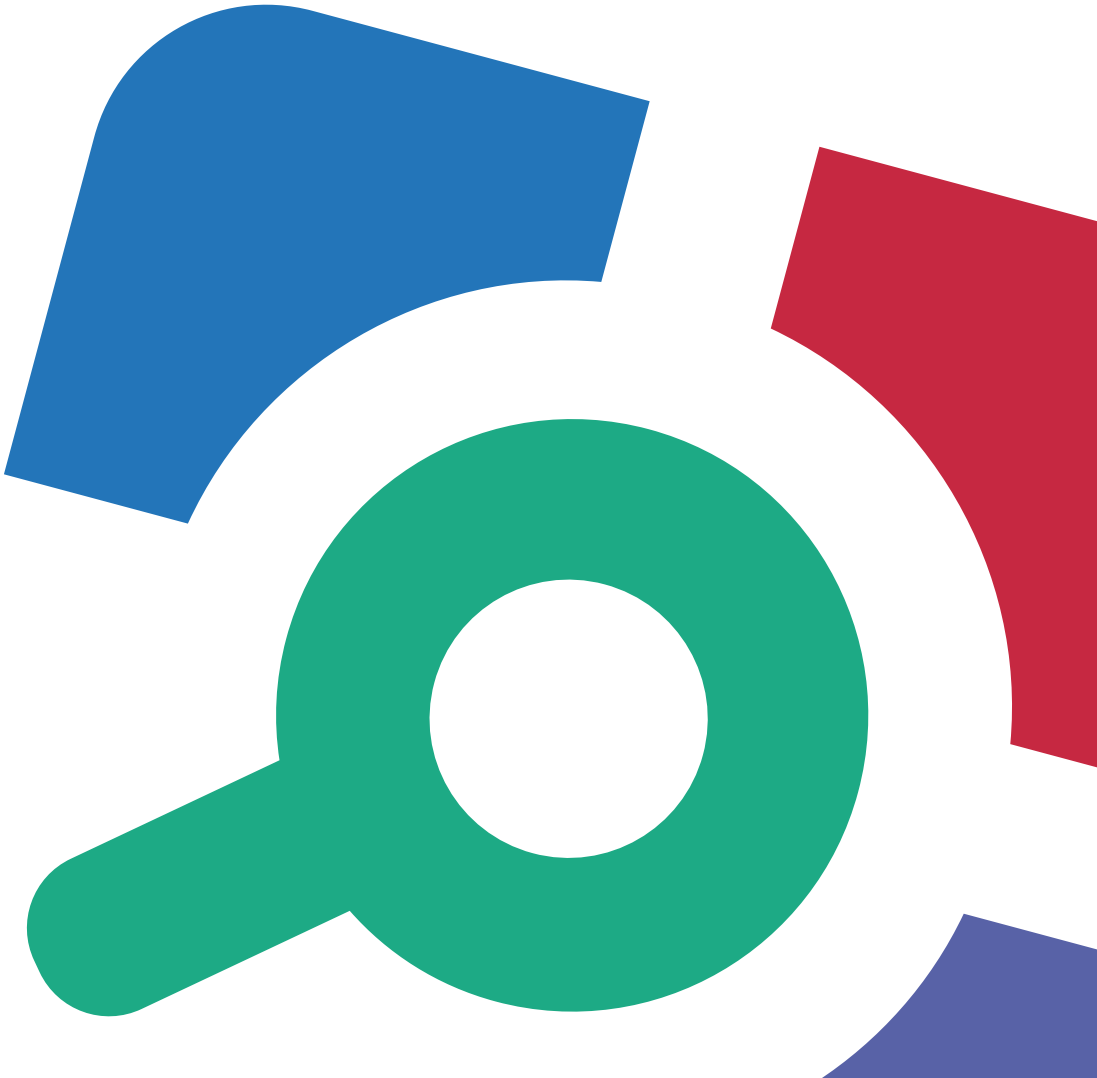
netwrix
#1 for change auditing

Netwrix Auditor

Installation and Configuration 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

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 event log data and rich reporting capabilities.

Netwrix Auditor Feature	Description
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 analyze how changes to your IT infrastructure are made. Netwrix Auditor allows searching inside video recordings and jumping to a

Netwrix Auditor Feature	Description
	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.

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 • 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

Netwrix Auditor Feature	Supported Versions
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 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

3. Install Netwrix Auditor

This chapter lists all software and hardware requirements for the Netwrix Auditor installation, recommendations on how to deploy the product and step-by-step instructions on how to install Netwrix Auditor and its agents.

Refer to the following sections for detailed information:

- Deployment Options
- System Requirements
- Install the Product
- Install Netwrix Auditor Agents

3.1. Deployment Options

This section provides recommendations on how best to deploy Netwrix Auditor. Review these recommendations and choose the most suitable option depending on which Netwrix Auditor features you are going to use.

Feature	Deployment Options
Active Directory Auditing Group Policy Auditing Exchange Server Auditing Inactive User Tracking	The product can be installed on any computer in the monitored domain. If you want to monitor several domains, you must establish two-way trust relationships between these domains and the domain where the product is installed.
Mailbox Access Auditing	The product can be installed on any computer in the forest, but it is not recommended to install it on a domain controller. If you want to monitor Exchange servers located in different forests, a separate instance of Netwrix Auditor must be installed in each forest.
Windows Server Auditing	The product can be installed on any computer in the domain or a workgroup where the monitored servers are located. If you want to monitor servers located in different domains, you must establish two-way trust relationships between these domains and the domain where the product is installed. If you want to monitor servers located in different workgroups, the monitored server(s) must have accounts with the same name and password as the account under which the product is run. Both accounts

Feature	Deployment Options
	must belong to the **Local Administrators** group.
Event Log Management VMware Auditing	The product can be installed on any computer in the monitored network.
User Activity Video Recording	The product can be installed on any computer in the domain where monitored computers are located. If you want to monitor computers located in different domains, you must establish two-way trust relationships between these domains and the domain where the product is installed.
Windows File Server Auditing NetApp Filer Auditing EMC Storage Auditing	Can be installed on any computer in the domain where the monitored file servers are located. If you want to monitor file server(s) located in different domains, the monitored file server(s) must have accounts with the same name and password as the account under which the product is run. Both accounts must belong to the **local Administrators** group.
SQL Server Auditing	Can be installed on any computer in the domain where the monitored SQL Servers are located. If you want to monitor SQL Servers located in different domains, the monitored servers must have an account with the same name and password as the account under which the product is run. This account must have the **sysadmin** role on the monitored SQL server and be a member of the **Local Administrators** group on the computer where the product is installed.
Password Expiration Alerting	Can be installed on any computer in the monitored domain.
SharePoint Auditing	Can be installed on any computer in the domain where the SharePoint Farms is located. If you want to monitor SharePoint Farms located in different domains, you must establish two-way trust relationships between these domains and the domain where the product is installed. The computer where Netwrix Auditor is installed must be able to access the Central Administration website on the audited SharePoint Farm by its name and port number . Netwrix Auditor Agent for SharePoint must be installed on the computer where SharePoint Central Administration is installed.

3.2. System Requirements

3.2.1. Hardware Requirements

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

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2GHz	Intel Core 2 Duo 2x 64 bit, 3GHz
Memory	2 GB RAM	8 GB RAM
Disk Space	1 TB	
Screen resolution	1024 x 768	Screen resolution recommended by your screen manufacturer.

3.2.2. Software Requirements

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

Component	Requirements
Operating system	• Windows 7 (32 and 64-bit) and above
.Net Framework	• .Net Framework 3.5 SP1
Additional Software	• Internet Explorer 7 and above • Windows Installer 3.1 and above • Windows Media Player (only required for the User Activity Video Recording feature) • Windows PowerShell 2.0 (only required for the Exchange Server Auditing feature if the target domain has an Exchange organization running Exchange Server 2010 or 2013) • Group Policy Management Console (only required for the Group Policy Auditing feature)

3.2.3. Supported Microsoft SQL Server Versions

Microsoft SQL Server provides the Reporting Services that enable creating reports based on data stored in a SQL Server database. Netwrix Auditor uses Microsoft SQL Server Reporting Services to generate reports on changes to the audited environment and on the point-in-time configuration.

To use the Reports functionality, Microsoft SQL Server must be deployed on the same computer where Netwrix Auditor is installed, or on a computer that can be accessed by the product.

The following Microsoft SQL Server versions are supported:

Version	Edition
SQL Server 2008	Express Edition with Advanced Services Standard or Enterprise Edition
SQL Server 2008 R2	Express Edition with Advanced Services Standard or Enterprise Edition
SQL Server 2012	Express Edition with Advanced Services Standard or Enterprise Edition

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.

Microsoft SQL Server is not included in the product installation package and must be installed manually or automatically through the Reports Configuration wizard. This wizard automatically installs SQL Server Express Edition with Advanced Services and configures the Reporting Services. The SQL Server version installed through the wizard depends on the operating system your computer is running:

SQL Server version	OS version
SQL Server 2008 R2 Express Edition with Advanced Services	• Windows 7 • Windows Server 2008 R2
SQL Server 2012 Express Edition with Advanced Services	• Windows Server 2008 R2 SP1 and above • Windows 7 SP1 • Windows 8 and above • Windows Server 2012 and above

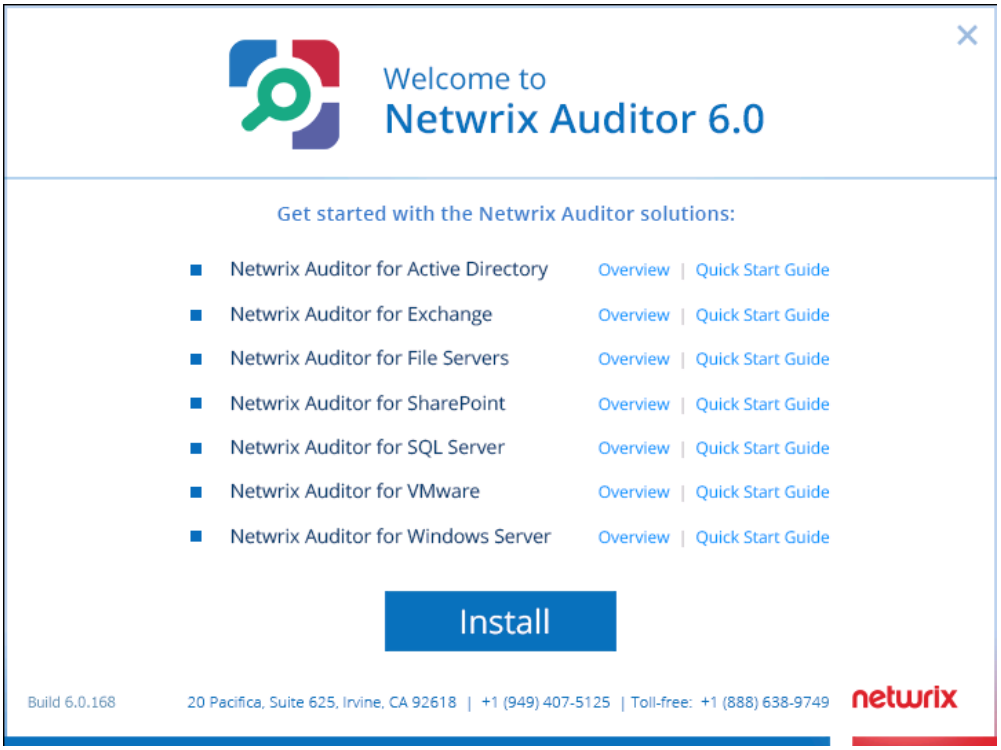
For your convenience, we have provided instructions on the manual installation of Microsoft SQL Server with Advanced Services. See Install Microsoft SQL Server for more information. For full installation and configuration details, refer to the documentation provided by Microsoft.

NOTE: If you install Netwrix Auditor on a read-only domain controller, SQL Server installation will fail (both manual or automatic through the Reports Configuration wizard). This is a known issue, for details refer to the following Microsoft Knowledge Base article: You may encounter problems when installing SQL Server on a domain controller. To fix the issue, install Netwrix Auditor on another computer, or install SQL Server manually on a different computer that can be accessed by the product.

3.3. Install the Product

To install Netwrix Auditor

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



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

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

3.4. Install Netwrix Auditor Agents

For most audited systems, Netwrix offers both agent-based and agentless data collection methods. The use of agents is recommended for distributed deployments or multi-site networks due to their ability to reduce network traffic, since data is transferred in a highly compressed format. If the agent-based data collection method is selected on Managed Object creation, agents are installed automatically on the audited computers.

The SharePoint Auditing and the User Activity Video Recording features only employ the agent-based data collection method and include native agents that must be installed in the audited environment to collect audit data. Both agents can be installed either automatically (on **New Managed Object** wizard completion), or manually.

Refer to the following sections below for manual installation instructions:

- Install Netwrix Auditor Agent for SharePoint
- Install Netwrix Auditor Agent for User Activity Video Recording

3.4.1. Install Netwrix Auditor Agent for SharePoint

Netwrix Auditor Agent for SharePoint must be installed in the audited SharePoint farm on the computer that hosts SharePoint Central Administration.

Before installing Netwrix Auditor Agent for SharePoint, make sure that:

- The **SPAdminV4** service is started on the target computer (See Configure Farm for SharePoint Auditing for more information.
- The user, under which the installation is going to be performed
  - is a member of the **local Administrators** group on the SharePoint server where the agent is going to be deployed
  - is granted the SharePoint_Shell_Access role in the SharePoint SQL Server configuration database. See Configure Data Processing Account Rights and Permissions for more information.

NOTE: Your SharePoint sites may be unavailable during the agent installation and uninstallation.

To install Netwrix Auditor Agent for SharePoint

1. Navigate to *%Netwrix Auditor installation folder%\Netwrix Auditor for SharePoint\ SharePointPackage* and copy **SpaPackage_<version>.msi** to the computer where Central Administration is installed,
2. Run the installation package.
3. Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.

3.4.2. Install Netwrix Auditor Agent for User Activity Video Recording

By default, the agent is installed automatically on the audited computers upon the **New Managed Object** wizard completion. If, for some reason, the installation has failed, you must install the agent manually on each of the audited computers.

Before installing Netwrix Auditor agent for User Activity Video Reporting, make sure that:

- The audit settings are configured properly See Configure Computers for User Activity Video Recording for more information.
- The Data Processing Account has access to the administrative shares (See Configure Data Processing Account Rights and Permissions for more information.

To install Netwrix Auditor agent for User Activity Video Recording

1. Navigate to *%Netwrix Auditor installation folder%\User Activity Video Reporter* and copy the **uavrfull_agent.msi** file to the audited computer.
2. Run the installation package.
3. Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.
4. On the **Agent Settings** page, specify the host server (i.e. the name of the computer where Netwrix Auditor is installed) and the server TCP port.

4. Configure IT Infrastructure for Audit

Netwrix Auditor relies on native logs for collecting audit data. Therefore, successful change auditing requires a certain configuration of the native audit settings in the audited environment and on the computer where Netwrix Auditor resides. Configuring your IT Infrastructure may also include enabling certain built-in Windows services, etc. Proper audit configuration is required to ensure audit data integrity, otherwise your change reports may contain warnings, errors or incomplete audit data.

The table below lists the native audit settings that must be adjusted to ensure collecting comprehensive and reliable audit data.

Feature	Required configuration
Active Directory Auditing Group Policy Auditing	***In the audited environment:*** • The ADSI Edit utility must be installed on any domain controller in the audited domain. See Install ADSI Edit for more information. • The **Audit account management** and the **Audit directory service access** policies must be set to *"Success"* for the effective domain controllers policy. • The **Audit logon events** policy must be set to *"Success"* (or *"Success"* and "*Failure"*) for the effective domain controllers policy. • The **Maximum Security event log** size must be set to 300MB on pre-Windows Vista versions, or to 4GB on Windows Vista and above. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*. OR Auto archiving must be enabled to prevent audit data loss if log overwrites occur. • Object-level audit settings must be configured for the **Domain**, **Configuration** and **Schema** partitions. • The AD **tombstoneLifetime** attribute must be set to *"730"*. ***On the computer where Netwrix Auditor is installed*** • Customize the retention period for the backup logs if necessary (by default, it is set to *"50"*).

Feature	Required configuration
Exchange Server Auditing	***In the audited environment:*** • The ADSI Edit utility must be installed on any domain controller in the audited domain. See Install ADSI Edit for more information. • The **Audit account management** and the **Audit directory service access** policies must be set to *"Success"* for the effective domain controllers policy. • The **Audit logon events** policy must be set to *"Success"* (or *"Success"* and "*Failure"*) for the effective domain controllers policy. • The **Maximum Security event log** size must be set to 300MB on pre-Windows Vista versions, or to 4GB on Windows Vista and above. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*. OR Auto archiving must be enabled to prevent audit data loss if log overwrites occur. • Object-level audit settings must be configured for the **Domain**, **Configuration** and **Schema** partitions. • The AD **tombstoneLifetime** attribute must be set to *"730"*. • Administrator Audit Logging settings must be configured (only required for Exchange Server 2010 and 2013). ***On the computer where Netwrix Auditor is installed*** • Customize the retention period for the backup logs, if necessary (by default, it is set to *"50"*).
Mailbox Access Auditing	***In the audited environment:*** • The **Logons** logging level must be set to *"Minimum"* via the Exchange Management Shell. **NOTE:** This is only required if you select the agentless data collection method.
Windows File Server Auditing	***In the audited environment:*** • The following options must be set to *"Successful"* and *"Failed"* in the **Advanced Security** settings for the audited shared folders: • List Folder / Read Data

Feature	Required configuration
	• Create Files / Write Data • Create Folders / Append Data • Write Attributes • Write Extended Attributes • Delete Subfolders and Files • Delete • Change Permissions • Take Ownership • The **Audit object access** policy must set to *"Success"* and *"Failure"*. • The Advanced audit policy settings must be configured if you want to narrow the scope of events collected by the product. • The **Security event log maximum size** must be set to 300MB on pre-Windows Vista versions, or to 4GB on Windows Vista and above. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*. • The **Remote Registry** service must be started.
NetApp Filer Auditing	***In the audited environment:*** • CIFS Network Protocol support is required. • Qtree Security must be configured. The volume where the audited file shares are located must be set to the *"ntfs"* security style. • The `httpd.admin.enable` or the `httpd.admin.ssl.enable` option must be set to *"on"*. For security reasons, it is recommended to configure SSL access and enable the `httpd.admin.ssl.enable` option. • The `cifs.audit.enable` and the`cifs.audit.file_access_events.enable` options must be set to *"on"*. • Unless you are going to audit logon events, the `cifs.audit.logon_events.enable` and the `cifs.audit.account_mgmt_events.enable` options must be set to *"off"*. • Security Log must be configured: • `cifs.audit.logsize 300 000 000 (300 MB)`

Feature	Required configuration

	• `cifs.audit.autosave.onsize.enable on`
	• `cifs.audit.autosave.file.extension timestamp`
	• Security Log Shared Folder must be specified.
	• Audit settings must be configured for CIFS File Shares:
	  • *"Successful"* and *"Failed"* must be selected next to:
	  • List Folder / Read Data
	  • *"Successful"* must be selected next to the following options:
	  • Create Files / Write Data
	  • Create Folders / Append Data
	  • Write Attributes
	  • Write Extended Attributes
	  • Delete Subfolders and Files
	  • Delete
	  • Change Permissions
	  • Take Ownership

EMC Storage Auditing	***In the audited environment:***
	• CIFS Network Protocol support is required.
	• **Security Event Log Maximum Size** must be set to 4GB.
	• The **Audit object access** policy must be set to *"Success"* and *"Failure"* in the Group Policy of the OU where the audited EMC VNX/VNXe/Celerra appliance belongs to.
	• Audit settings must be configured for CIFS File Shares. *"Successful"* and *"Failed"* must be set next to the following options:
	  • List Folder / Read Data
	  • Create Files / Write Data
	  • Create Folders / Append Data
	  • Write Attributes
	  • Write Extended Attributes
	  • Delete Subfolders and Files

Feature	Required configuration
	• Delete • Change Permissions • Take Ownership

Windows Server Auditing	***In the audited environment:***
	• The **Remote Registry** and the **Windows Management Instrumentation (WMI)** service must be started.
	• The following audit policies must be configured depending on the OS:
	  • On pre-Windows Vista: the **Audit account management** and the **Audit object access** policy must be set to *"Success"*.
	  • On Windows Vista and above: the **Audit Security Group Management, Audit User Account Management, Audit Handle Manipulation, Audit Other Object Access Events** and **Audit Registry** policy must be set to *"Success"*.
	• The **Security event log maximum size** must be set to 300 MB on pre-Windows Vista versions, or to 4 GB on Windows Vista and above. The retention method of the **Security event log** must be set to *"Overwrite events as needed"*.
	
	NOTE: If the audited servers are behind the Firewall, for configuration details refer to the following Netwrix Knowledge Base articles: How to audit servers located in another subnet behind firewall and Ports required to monitor servers over the firewall.

Event Log Management	***In the audited environment:*** • For Windows-based platforms: the **Remote Registry** service must be running and its **Startup Type** must be set to *"Automatic"*. • For Syslog-based platforms: the Syslog daemon must be configured to redirect events.
User Activity Video Recording	***In the audited environment:*** • The **Windows Management Instrumentation** and the **Remote Registry** service must be running and their **Startup Type** must be set to *"Automatic"*. • The **File and Printer Sharing** and the **Windows Management Instrumentation** features must be allowed to communicate

Feature	Required configuration
	through Windows Firewall. • Local TCP Port 9003 must be opened for inbound connections. • Remote TCP Port 9002 must be opened for outbound connections. *On the computer where Netwrix Auditor is installed:* • The **Windows Management Instrumentation** and the **Remote Registry** services must be running and their **Startup Type** must be set to *"Automatic"*. • The **File and Printer Sharing** and the **Windows Management Instrumentation** features must be allowed to communicate through Windows Firewall. • Local TCP Port 9002 must be opened for inbound connections.
SharePoint Auditing	*In the audited environment:* • The **Audit Log Trimming** setting must be set to *"Yes"* and **Specify the number of days of audit log data to retain** must be set to 7 days. • The **Editing users and permissions** option must be enabled. • The **SPAdminV4** service must be enabled (required for the Netwrix Auditor Agent for SharePoint installation). *On the computer where Netwrix Auditor is installed:* • The **NetTcpPortSharing** service must be enabled.
SQL Server Auditing	No configuration is required
VMware Auditing	No configuration is required
Inactive User Tracking	No configuration is required
Password Expiration Alerting	No configuration is required

Refer to the following topics for detailed instructions depending on the system you are going to audit:

- Configure Domain for Active Directory Auditing
- Configure Domain for Group Policy Auditing
- Configure Domain for Exchange Server Auditing

- Configure Exchange Server for Mailbox Access Auditing
- Configure Servers for Windows File Server Auditing
- Configure Infrastructure for NetApp Filer Auditing
- Configure Infrastructure for EMC Storage Auditing
- Configure Infrastructure for Windows Server Auditing
- Configure Infrastructure for Event Log Management
- Configure Computers for User Activity Video Recording
- Configure Farm for SharePoint Auditing

4.1. Configure Domain For Active Directory Auditing

You can configure your domain for Active Directory Auditing in one of the following ways:

- Automatically when creating a Managed Object.

  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.

- Automatically through the **Active Directory Audit Configuration** wizard.

  With this wizard you can configure audit settings for the Active Directory Auditing, Group Policy Auditing and Exchange Server Auditing features.

  On each step, the wizard checks your audit settings and provides a report on their current values. If any of your current settings conflict with the configuration required for the product to function properly, any such conflicts will be listed. In this case, you can choose whether you want to adjust your audit settings automatically and override your current settings, or if you want to configure them manually. For instructions, refer to Configure Audit Automatically with Active Directory Audit Configuration Wizard

- Manually. See Configure Audit Manually for more information.

4.1.1. Configure Audit Automatically with Active Directory Audit Configuration Wizard

You can configure audit settings in the target Active Directory domain automatically, through the **Active Directory Audit Configuration** wizard. With this wizard you can configure audit settings for the Active Directory Auditing, Group Policy Auditing and Exchange Server Auditing features.

To configure audit automatically through the Active Directory Audit Configuration wizard

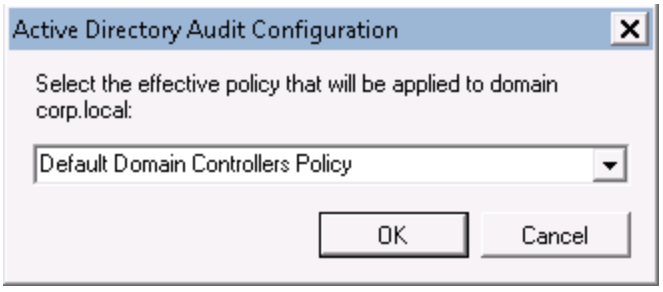
NOTE: For the wizard to work properly, you must run it under an account that is a member of the **domain Administrators** or **enterprise Administrators** group.

1. Launch the **Active Directory Audit Configuration** wizard. Navigate to *%Netwrix Auditor installation folder%\ AD Change Reporter Full Version*. Locate the Active Directory Audit Configuration shortcut and double-click it to launch the wizard.
2. On the first step, specify the name of the domain that you want to configure for audit.

3. Enable the **Apply to the forest root domain** option if you want to monitor changes to Active Directory schema and configuration, as the forest root domain contains audit settings for the Configuration and Schema partitions.

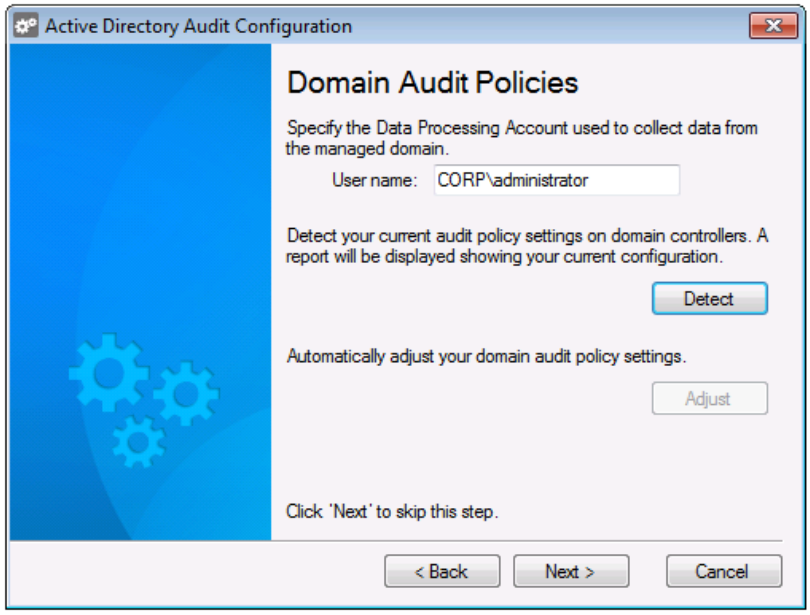
   NOTE: Monitoring of the Configuration partition is enabled by default. For instructions on how enable monitoring of changes to the Scema partition, refer to Netwrix Auditor Administrator's Guide.

4. Select the effective policy that is currently applied to the domain controllers and that is subject to change.

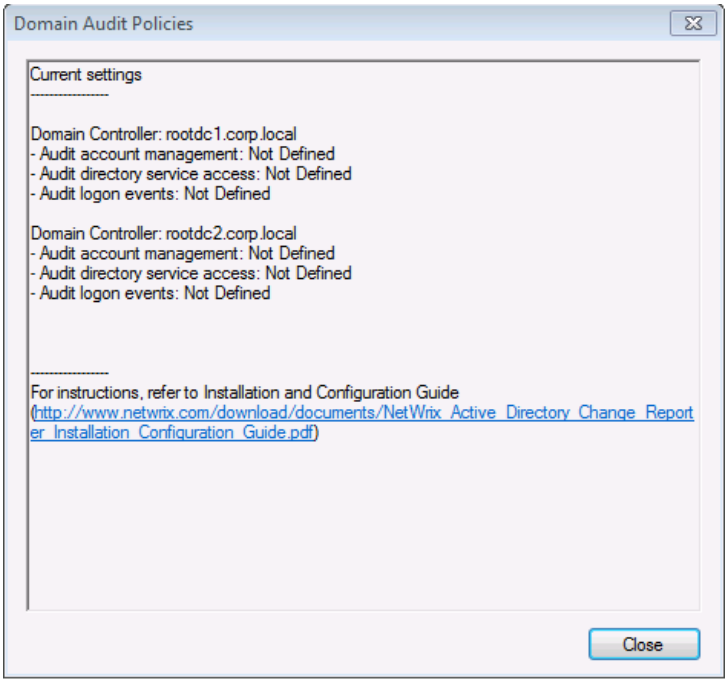


5. On the **Domain Audit Policies** step, specify the **Data Processing Account** that will be used by

Netwrix Auditor to collect data from the audited domain.



6. Click **Detect.** If your current settings do not match the configuration required for the product to function properly, a report will be displayed showing the current audit policy settings in the monitored domain as in the example below:



NOTE: If any of your other policies conflict with the settings required for the product to function properly, a warning message will be displayed listing these conflicts. If this happens, analyze carefully how your environment will be affected before applying the required settings.

To apply the required configuration automatically, click **Adjust**. Your audit policy settings and the **Manage auditing and security log** right will be adjusted and the confirmation dialog will be displayed on successful operation completion.

7. On the **Object-Level Audit Settings** step, click **Detect** to verify your object-level audit settings for the Domain, Configuration and Schema partitions. Click **Adjust** to configure the required settings automatically.

8. On the **Event Log Size and Retention Settings** step, click **Detect** to verify your **Security event log** size and retention settings. Click **Adjust** to configure the required settings automatically.

9. On the **Exchange Server Administrator Audit Logging Settings** step, click **Detect** to verify your Exchange Server Administrator Audit Logging settings. Click **Adjust** to configure the required settings

automatically.

NOTE: This step is required only if the audited AD domain has an Exchange organization running Microsoft Exchange Server 2010 or 2013. Otherwise, skip this step.

10. Review your audit settings and complete the wizard.

4.1.2. Configure Audit Manually

To configure your domain for Active Directory Auditing manually, perform the following procedures:

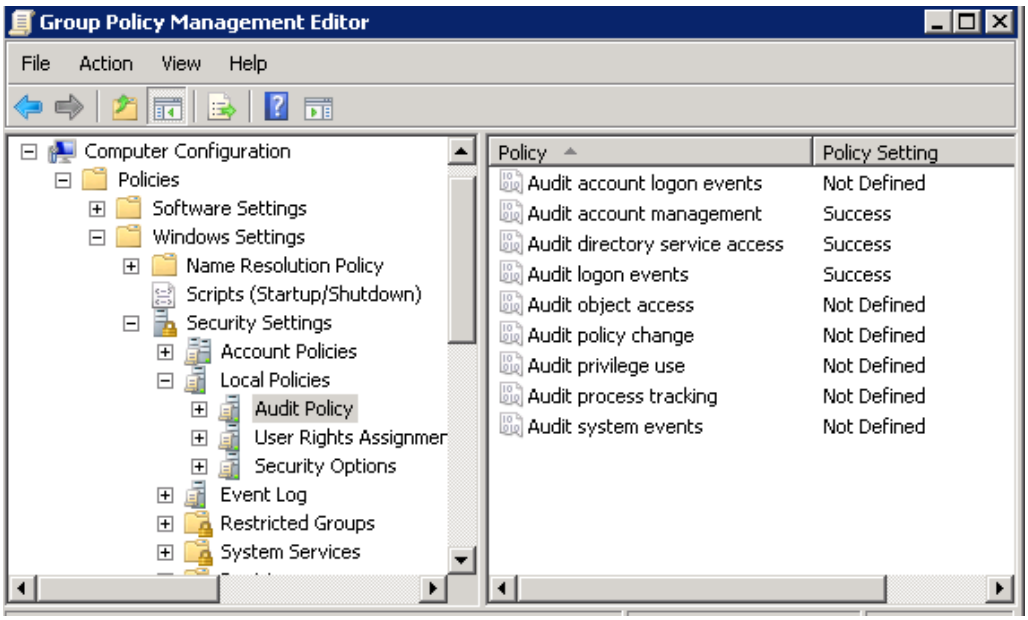
- Configure Domain Audit Policies
- Configure Security Event Log Size and Retention Settings
- Configure Object-Level Auditing
- Adjust Active Directory Tombstone Lifetime

4.1.2.1. Configure Domain Audit Policies

The domain audit policies must be configured to track changes to accounts and groups and to identify the workstation from which a change was made.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the

left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy.**

4. Set the **Audit account management** and the **Audit directory service access** policy to *"Success"*. Set the **Audit logon events** policy to *"Success"* (or *"Success"* and *"Failure"*).
5. 

NOTE: The **Audit logon events** policy is only required to collect the information on the originating workstation, i.e. the computer from which a change was made. This functionality is optional and can be disabled (for instructions refer to Netwrix Auditor Administrator's Guide).

6. Navigate to **Start** → **Run** and type *'"cmd"*. Input the `gpupdate /force` command and click **Enter**. The group policy will be updated.

4.1.2.2. Configure Security Event Log Size and Retention Settings

Defining the **Security event log** size is essential for change auditing. If your Security log size is insufficient, overwrites may occur before data is written to the Audit Archive and the SQL database, and some audit data may be lost. To prevent overwrites, you must increase the maximum size of the **Security event log**.

On Windows Server 2003 systems, where the maximum size of the **Security event log** cannot exceed 300 MB (according to the following Microsoft Knowledge Base article: Event log may not grow to configured size), it is also recommended to enable automatic backup of the event log. With this option, the event log will be archived and log overwrites will not occur on domain controllers.

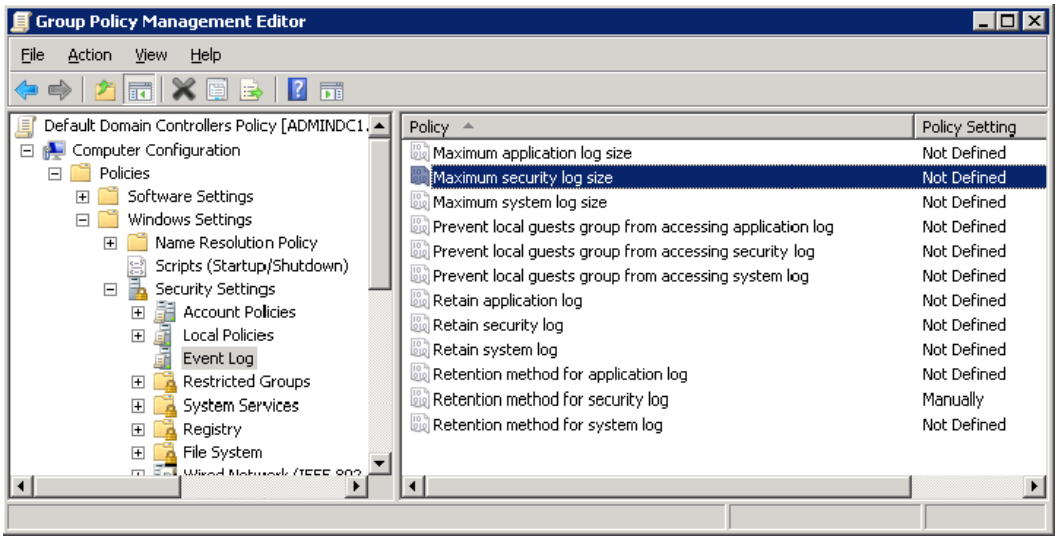
The retention method of the **Security event log** must be set to *"Overwrite events as needed"* (unless it is set to *"Archive the log when full"*). In this case, events will be written into the log even if it reaches its maximum size (new events will overwrite the oldest events in the log). Alternatively, you can enable auto archiving for the **Security event log** to prevent audit data loss if log overwrites occur.

To adjust your **Security event log** size and retention settings, perform the following procedures:

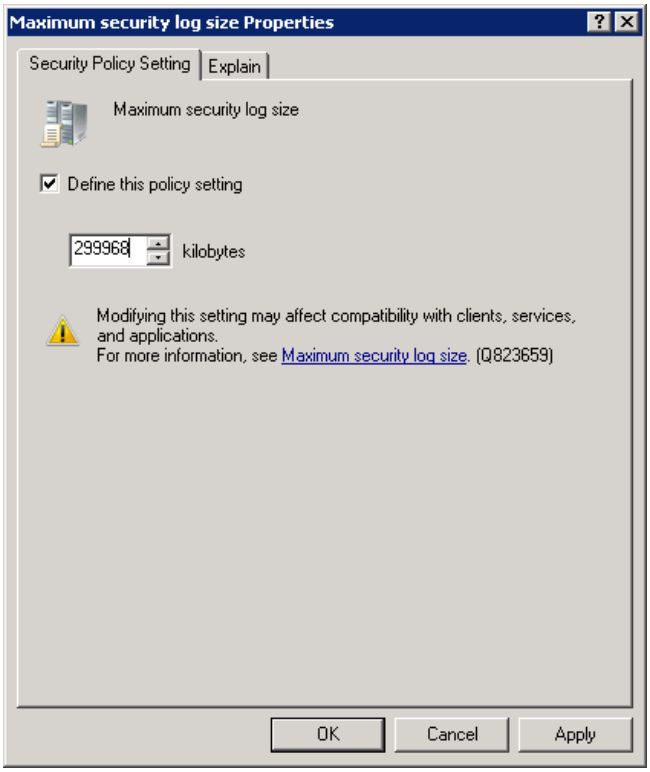
- To increase the maximum size of the Security event log and set its retention method
- To enable Auto archiving centrally on all domain controllers
- To configure the retention period for the backup logs

To increase the maximum size of the Security event log and set its retention method

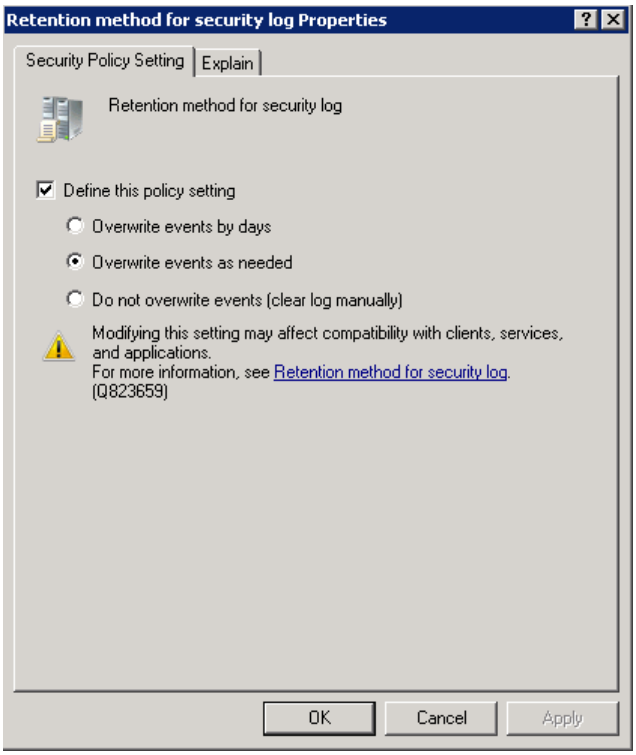
1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. Navigate to **Computer Configuration** → **Policies** → **Windows Settings** →**Security Settings** → **Event Log** and double-click the **Maximum security log size** policy.



4. In the **Maximum security log size Properties** dialog, select **Define this policy setting** and set maximum security log size to *"299968"* kilobytes (300MB) on pre-Windows Vista versions, or to *"4194304"* kilobytes (4GB) on Windows Vista and above.



5. Select the **Retention method for security log** policy. In the **Retention method for security log Properties** dialog, check **Define this policy** and select **Overwrite events as needed**.



6. Navigate to **Start** → **Run** and type *'"cmd"*. Input the `gpupdate /force` command and click **Enter**. The group policy will be updated.

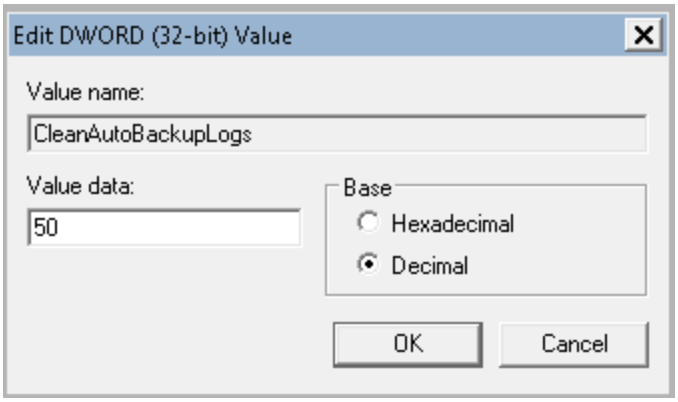
To enable Auto archiving centrally on all domain controllers

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. Navigate to **Computer Configuration** → **Policies**. Right-click **Administrative Templates: Policy definitions** and select **Add / Remove templates**. Click **Add** in the dialog that opens.
4. In the **Policy Templates** dialog, navigate to the Netwrix Auditor installation directory, open the **AD Change Reporter Full Version** folder and select the **Log Autobackup.adm** file (if the product is installed on a different computer, copy this file to the domain controller), and click **Open**.

   NOTE: If you are running Widows Server 2003 or below, click **View** in the main menu, select **Filtering** and clear **Only show policy settings that can be fully managed**.
5. Navigate to **Administrative Templates: Policy definitions** → **Classic Administrative Templates** → **System** → **Event Log**. Select **Automatically clear a full security event log and back up the log file** and set it to *"Enable"*.
6. Navigate to **Start** → **Run** and type *"cmd"*. Input the `gpupdate /force` command and click **Enter**. The group policy will be updated.

To configure the retention period for the backup logs

1. On the computer where **Netwrix Auditor** is installed, open the Registry Editor: navigate to **Start**→ **Run** and type *"regedit"*.
2. Depending on your OS, navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Netwrix** → **AD Change Reporter** (for 32-bit OS), or **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix** → **AD Change Reporter** (for 64-bit OS).
3. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open. This value defines the time period (in hours) after which security event logs archives will be automatically deleted from the domain controllers. By default, it is set to *"50"* (decimal). Modify this value, if necessary, and click **OK** to save the changes.



NOTE: If the **CleanAutoBackupLogs** registry value is set to *"0"*, you will have to remove the old automatic backups manually, or you may run out of space on your hard drive.

4.1.2.3. Configure Object-Level Auditing

Object-level Active Directory auditing must be configured so that the "Who" and "When" information appears in audit reports. If, in addition to the Domain partition, you also want to monitor changes to AD configuration and schema, you must enable object-level auditing for these partitions.

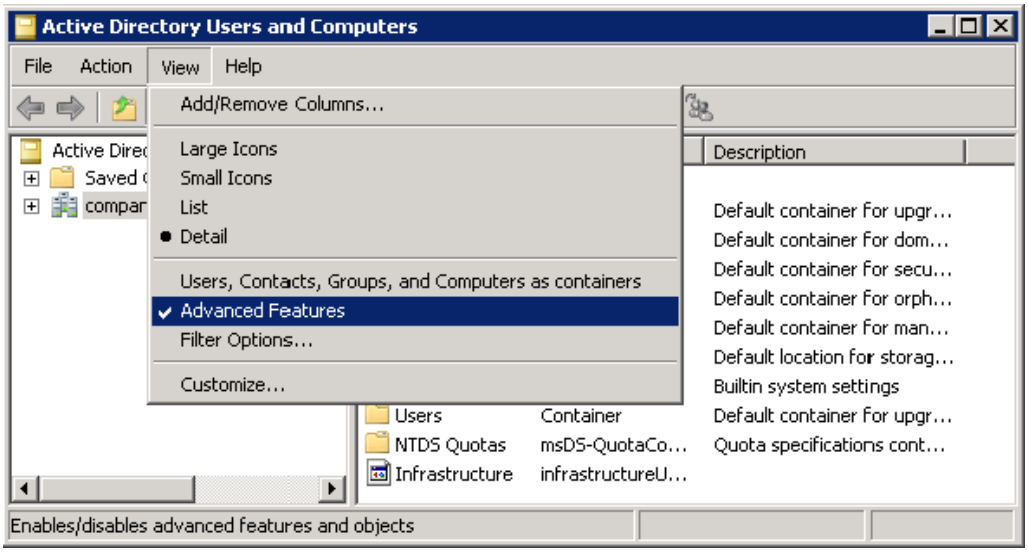
NOTE: Monitoring of the Configuration partition is enabled by default. Refer to Netwrix Auditor Administrator's Guide for detailed instructions on how to enable monitoring of changes to the Schema partition in the target AD domain.

Perform the following procedures to configure object-level auditing for the Domain, Configuration and Schema partitions:

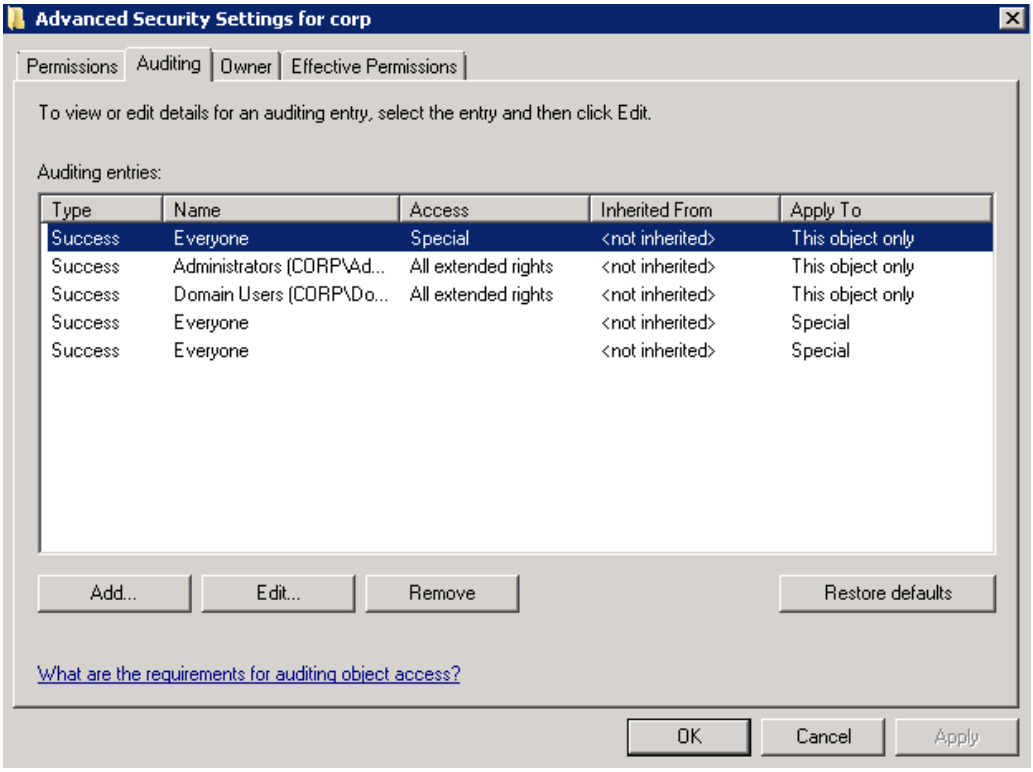
- To configure object-level auditing for the Domain partition
- To enable object-level auditing for the Configuration and Schema partitions

To configure object-level auditing for the Domain partition

1. Open the **Active Directory Users and Computers** console on any domain controller in the target domain: Navigate to **Start** → **Administrative Tools** → **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** dialog, click **View** in the main menu and ensure that the **Advanced Features** are enabled.



3. Right-click the **<domain_name>** node and select **Properties.** Select the **Security** tab and click **Advanced**. In the **Advanced Security Settings** dialog select the **Auditing** tab.

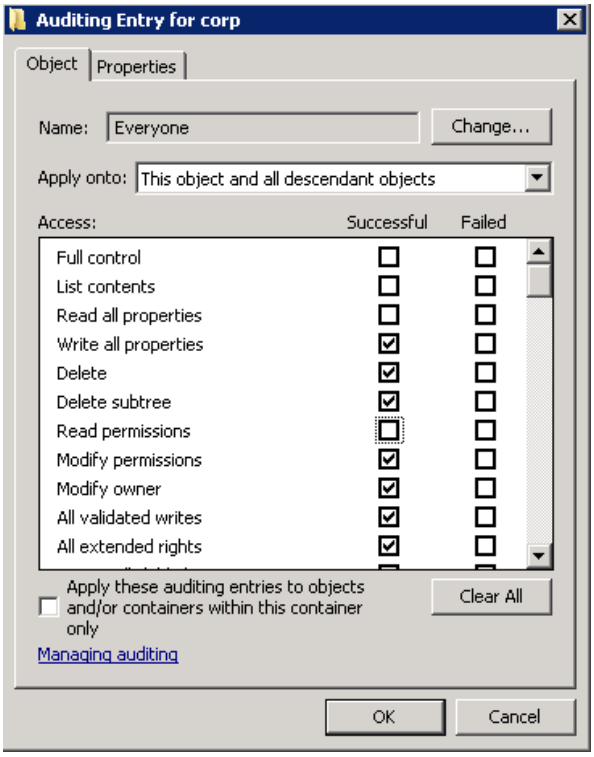


4. Do one of the following: depending on the OS:

   - On pre-Windows Server 2012 Windows versions:

     a. Click **Add**. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

     b. In the **Audit Entry** dialog that opens, set the *"Successful"* parameter for all access entries except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.



c. Make sure that **Apply these auditing entries to objects and/or containers within this container only** check-box is cleared. Also, make sure that the **Apply onto** parameter is set to *"This object and all descendant objects"*.

- On Windows Server 2012 and above

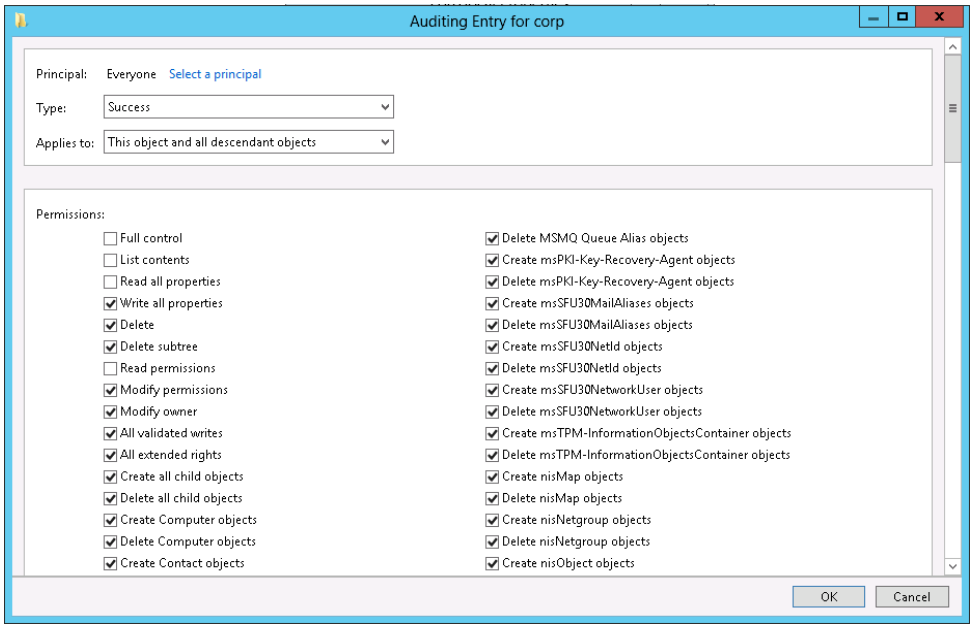
a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

b. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

c. Set **Type** to *"Success"* and **Applies to** to *"This object and all descendant objects"*.

d. Under **Permissions**, select all check-boxes except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.

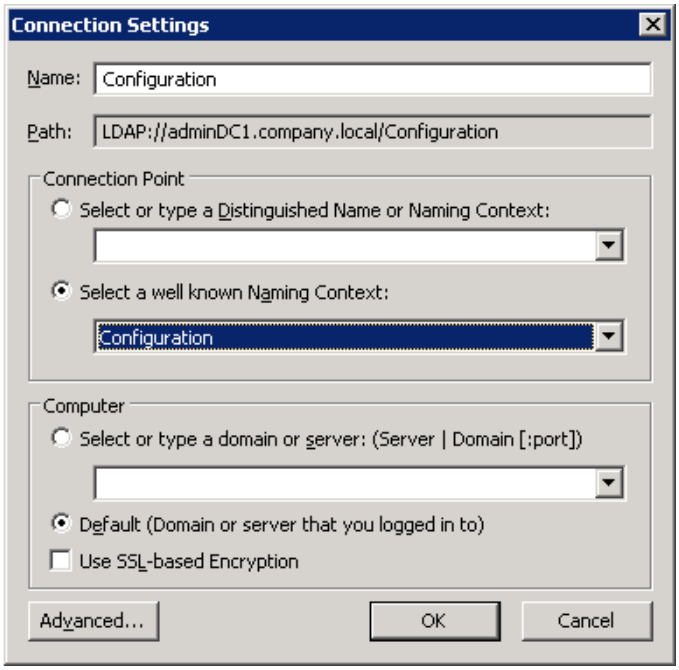
e. Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container** check-box is cleared.



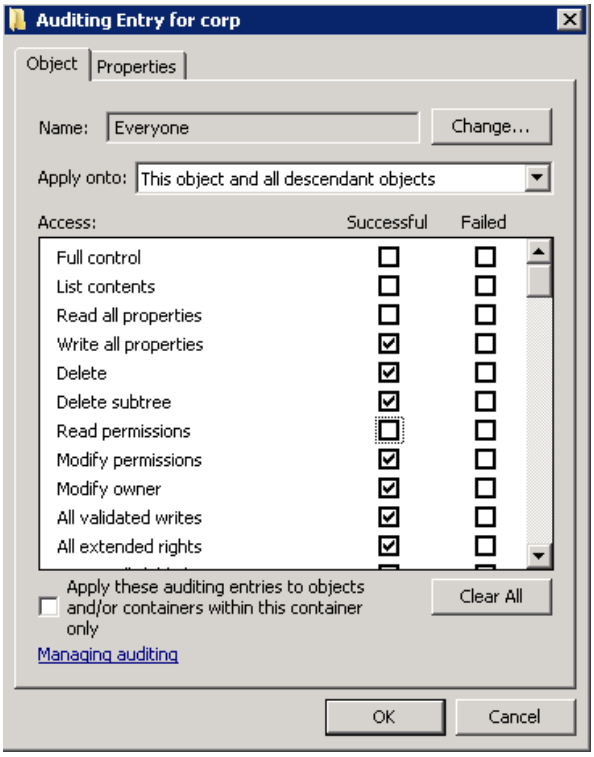
To enable object-level auditing for the Configuration and Schema partitions

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. Refer to Install ADSI Edit for detailed instructions on how to install the ADSI Edit utility.

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 **Configuration** from the drop-down list.



3. Expand the **Configuration <Your_Root_Domain_Name>** node. Right-click the **CN=Configuration, DC=<name>,DC=<name>...** node and select **Properties.**
4. In the **CN=Configuration, DC=<name>, DC=<name> Properties** dialog select the **Security** tab and click **Advanced**. In the **Advanced Security Settings for Configuration** dialog open the **Auditing** tab.
5. Do one of the following: depending on the OS:
   - On pre-Windows Server 2012 Windows versions:
     a. Click **Add**. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.
     b. In the **Audit Entry** dialog that opens, set the *"Successful"* parameter for all access entries except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.



c. Make sure that **Apply these auditing entries to objects and/or containers within this container only** check-box is cleared. Also, make sure that the **Apply onto** parameter is set to *"This object and all descendant objects"*.

- On Windows Server 2012

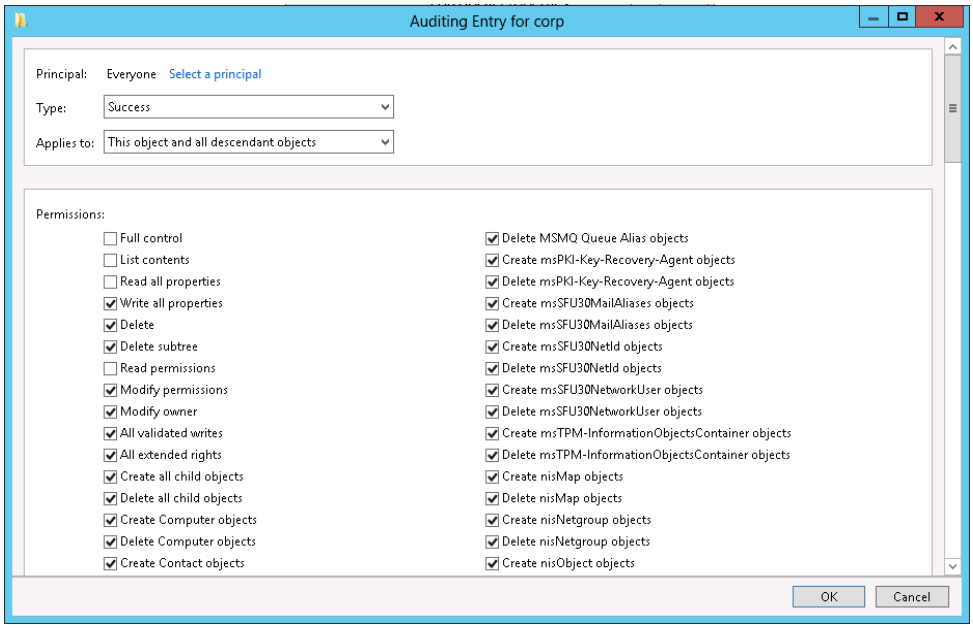
a. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.

b. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.

c. Set **Type** to *"Success"* and **Applies to** to *"This object and all descendant objects"*.

d. Under **Permissions**, select all check-boxes except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.

e. Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container** check-box is cleared.



6. Repeat these steps for the Schema container if necessary.

4.1.2.4. Adjust Active Directory Tombstone Lifetime

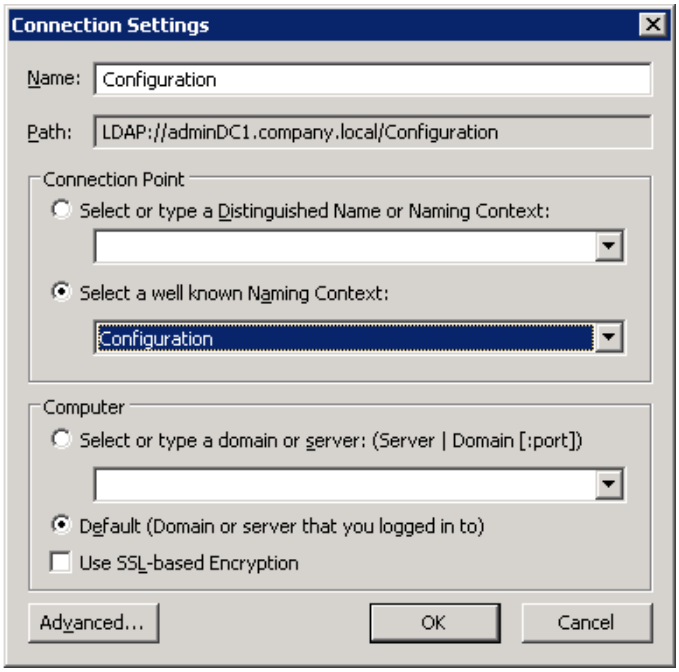
You can restore deleted Active Directory objects and their attributes using the Active Directory Object Restore tool integrated with Netwrix Auditor. The tool finds the information on deleted objects in the product snapshots (this data is stored in the Audit Archive, a local file-based storage of audit data) and AD tombstones.

To be able to restore deleted Active Directory objects, you must adjust the Active Directory tombstone lifetime property (set by default to 60 days in Windows Server 2003 and to 180 days in Windows Server 2008 and above) so that it agrees with the Audit Archive retention period (2 years by default).

To change the tombstone lifetime attribute

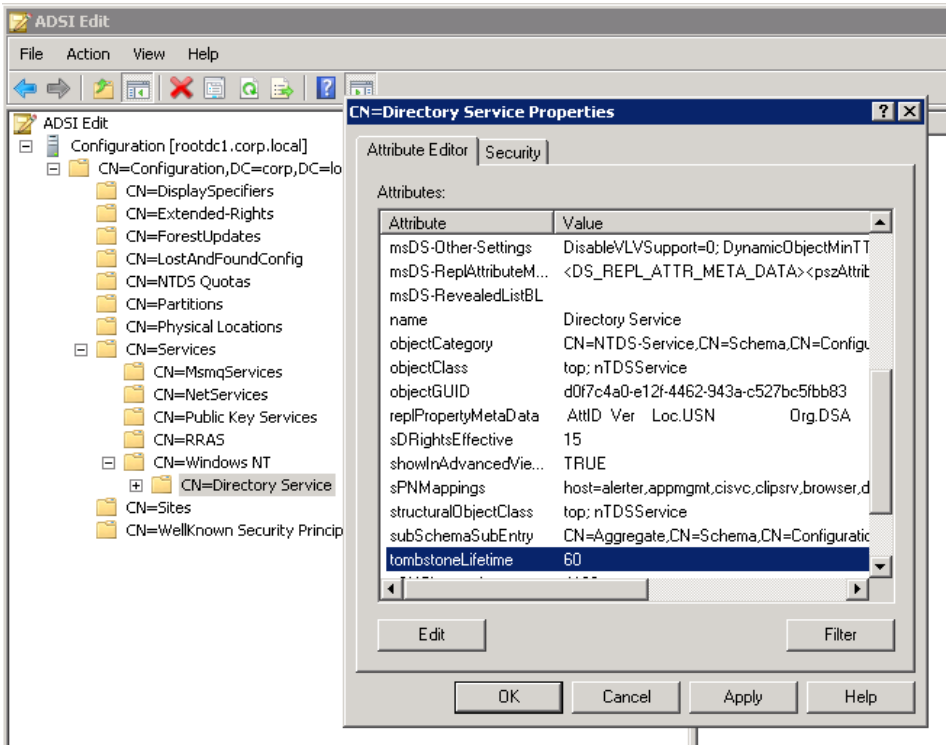
NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2003 systems, this utility is a component of Windows Server Support Tools. In Windows Server 2008 systems and above, this component is installed together with the AD DS role, or it can be downloaded and installed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

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 **Configuration** from the drop-down list.



3. Navigate to **Configuration <Your_Root_Domain_Name** → **CN=Configuration,DC=<name>,DC=<name>** → **CN=Services** → **CN=Windows NT** → **CN=Directory Service**. Right-click it and select **Properties** from the pop-up menu.

4. In the **CN=Directory Service Properties** dialogue, in the **Attribute Editor** tab locate the **tombstoneLifetime** attribute.



5. Click **Edit**. Set the value to *"730"* (which equals 2 years).

4.2. Configure Domain for Group Policy Auditing

You can configure your domain for Group Policy Auditing in one of the following ways:

- Automatically when creating a Managed Object.

  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.

- Automatically through the **Active Directory Audit Configuration** wizard.

  With this wizard you can configure audit settings for the Active Directory Auditing, Group Policy Auditing and Exchange Server Auditing features.

  On each step, the wizard checks your audit settings and provides a report on their current values. If any of your current settings conflict with the configuration required for the product to function properly, any such conflicts will be listed. In this case, you can choose whether you want to adjust your audit settings automatically and override your current settings, or if you want to configure them manually. For instructions, refer to Configure Audit Automatically with Active Directory Audit Configuration Wizard

- Manually. You need to adjust the same audit settings as for the Active Directory Auditing feature. See Configure Audit Manually for more information.

4.3. Configure Domain for Exchange Server Auditing

You can configure your domain for Exchange Server Auditing:

- Automatically when creating a Managed Object.

  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.

- Automatically through the **Active Directory Audit Configuration** wizard.

  With this wizard you can configure audit settings for the Active Directory Auditing, Group Policy Auditing and Exchange Server Auditing features.

  On each step, the wizard checks your audit settings and provides a report on their current values. If any of your current settings conflict with the configuration required for the product to function

properly, any such conflicts will be listed. In this case, you can choose whether you want to adjust your audit settings automatically and override your current settings, or if you want to configure them manually. For instructions, refer to Configure Audit Automatically with Active Directory Audit Configuration Wizard

- Manually. You need to adjust the same audit settings as for the Active Directory Auditing feature. See Configure Audit Manually for detailed instructions. If the audited Exchange Organization has Exchange Server 2010 or 2013, you must also configure the Administrator Audit Logging (AAL) Settings.

4.3.1. Configure Exchange Server Administrator Audit Logging Settings

If the audited AD domain has an Exchange organization running Microsoft Exchange Server 2010 or 2013, you must configure the Exchange server Administrator Audit Logging (AAL) settings. To do this, perform the following procedure on any of the audited Exchange servers (these settings will then be replicated to all Exchange servers in the domain)

To configure Exchange Server Administrator Audit Logging settings

1. On the computer where the audited Microsoft Exchange Server is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**.
2. Execute the following command depending on your Exchange Server version:
   - Exchange Server 2010

     ```
     Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
     AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets *
     ```

   - Exchange Server 2013

     ```
     Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
     AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets * -LogLevel Verbose
     ```

3. On the computer where Netwrix Auditor is installed, browse to the *%Netwrix Auditor installation folder%/Netwrix/AD Change Reporter Full Version* folder, locate the **SetAALExcludedCmdlets.ps1** file and copy it to the Exchange server.
4. In **Exchange Management Shell**, in the command line, execute this file by specifying the path to it:

   ```
   <Path_To_ SetAALExcludedCmdlets_File>\SetAALExcludedCmdlets.ps1
   ```

   This file contains a list of cmdlets that must be excluded from Exchange Server logging to reduce server load.

4.4. Configure Exchange Server for Mailbox Access Auditing

Netwrix Auditor allows auditing non-owner mailbox access on Exchange Server 2003, 2007 and 2010, and provides auditing agents that let you dispense with native Exchange Server auditing. Agents log the information on all types of non-owner activities in other users' mailboxes (opening messages and folders, sending emails, and so on). If agents are disabled, only the access event itself is logged.

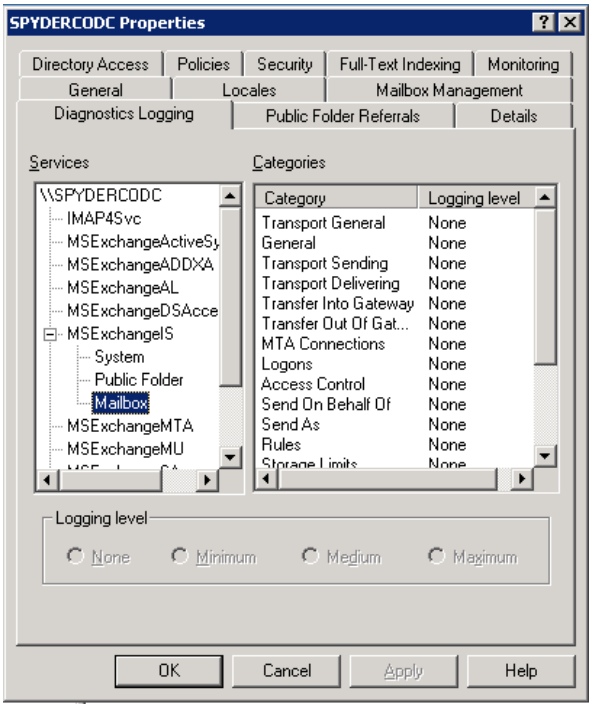
NOTE: Netwrix Auditor plans to support Mailbox Access Auditing on Exchange Server 2013 in the future releases.

If you choose the agentless data collection method, you must configure native auditing on the audited Exchange Servers. Do one of the following: depending on the OS:

- To configure Mailbox Access Auditing for Exchange Server 2003
- To configure Mailbox Access Auditing for Exchange Server 2007 and 2010

To configure Mailbox Access Auditing for Exchange Server 2003

1. On the computer where the audited Exchange Server is installed, navigate to **Start** → **All Programs** → **Microsoft Exchange** → **System Manager**.
2. In the **Exchange System Manager** dialog, in the left pane, navigate to your Exchange Server, right-click it and select **Properties** from the pop-up menu.
3. In the **Exchange Server Properties** dialog, select the **Diagnostics Logging** tab.
4. Under **Services**, navigate to **MSExchangeIS** → **Mailbox**.



5. Under **Categories**, select **Logons** and set its logging level to *"Minimum"*.
6. Navigate to **Start** → **Run** and type *"services.msc"*. In the Services snap-in, locate a service called **Microsoft Exchange Information Store** and restart it.

To configure Mailbox Access Auditing for Exchange Server 2007 and 2010

1. On the computer where the audited Microsoft Exchange Server is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**.
2. Execute the following command:

```
Set-EventLogLevel "MSExchangeIS\9000 Private\Logons" -Level Low
```

3. Navigate to **Start** → **Run** and type *"services.msc"*. In the Services snap-in, locate a service called **Microsoft Exchange Information Store** and restart it.

4.5. Configure Servers for Windows File Server Auditing

Before configuring the audit settings, consider that if you have multiple file shares frequently accessed by a significant number of users, it is reasonable to audit objects modification only. Tracking all access events may result in too much data written to the audit logs, whereas only some part of it may be of any interest. Note that audit flags must be set on every file share you want to audit.

If you are going to monitor an entire file server, consider the following:

- If you specify a single computer name, Netwrix Auditor will monitor all shared folders on this computer except the folders whose name ends with the $ symbol (which are either hidden or administrative/system folders). In order for the report functionality to work properly, you need to configure audit settings for each share folder on the computer separately. Otherwise, reports will contain limited data and warning messages.
- For your convenience, if your file shares are stored within one folder (or disk drive), you can configure audit settings for this folder only. As a result, you will receive reports on all required access types applied to all file shares within this folder. It is not recommended to configure audit settings for system disks.

To configure audit settings for Windows File Server Auditing, perform the following procedures:

- Configure Object-Level Access Auditing
- Configure Audit Object Access Policy
- Configure Event Log Size and Retention Settings
- Enable Remote Registry Service

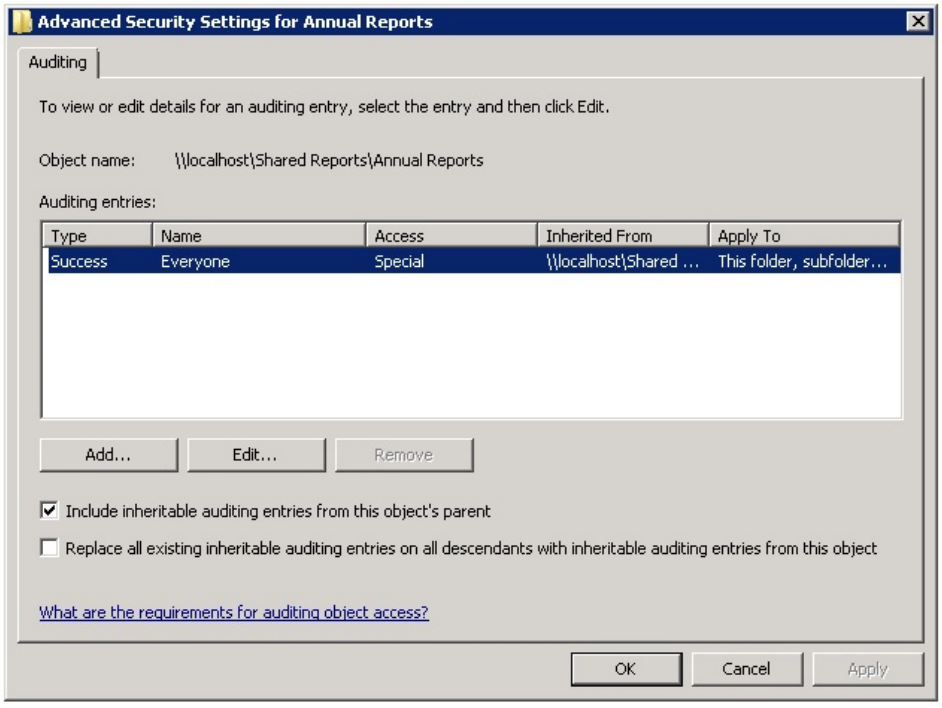
4.5.1. Configure Object-Level Access Auditing

Perform one of the following procedures depending on the OS:

- To configure Object-level access auditing on pre-Windows Server 2012 versions
- To configure Object-level access auditing on Windows Server 2012 and above

To configure Object-level access auditing on pre-Windows Server 2012 versions

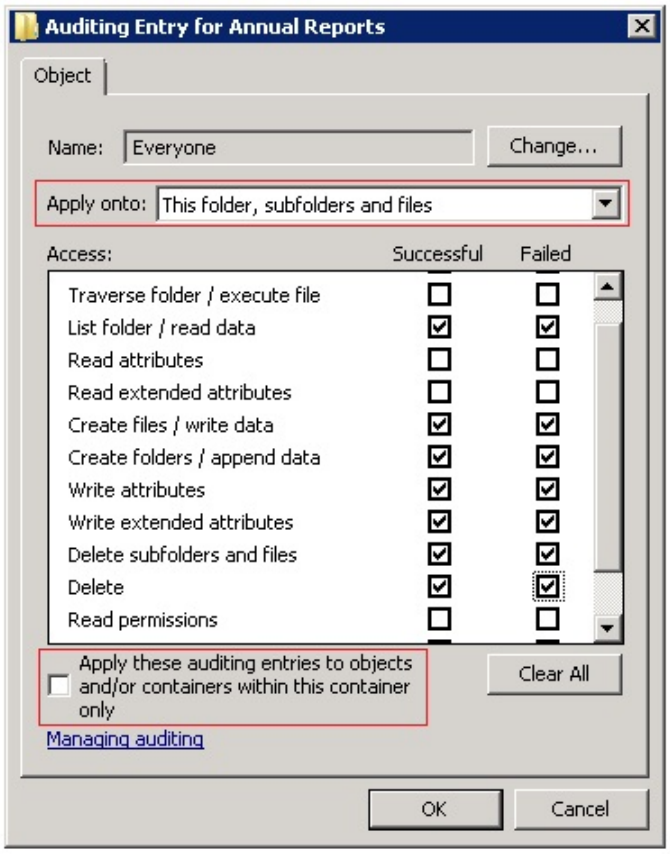
1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit.**
4. In a separate **Advanced Security Settings for <Share_Name>** dialog, select **Everyone** and click **Edit**.



NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the Reports functionality and the product will only monitor user accounts that belong to the selected group.

5. In the **Auditing Entry for <Share_Name>** dialog, select **Successful** and **Failed** next to the following options:

- To monitor successful read access and failed read access attempts:
  - List Folder / Read Data
- To monitor successful modifications and failed modification attempts:
  - Create Files / Write Data
  - Create Folders / Append Data
  - Write Attributes
  - Write Extended Attributes
  - Delete Subfolders and Files
  - Delete
  - Change Permissions
  - Take Ownership



6. Make sure that **Apply onto** is set to *"This folder, subfolders and files"*, and **Apply these auditing entries to objects and/or containers within this container only** is cleared.

To configure Object-level access auditing on Windows Server 2012 and above

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, select **Everyone** (or another user-defined group containing users that are granted special permissions) and click **Edit.**

   NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the Reports functionality and the product will only monitor user accounts that belong to the selected group.

4. In the **Auditing Entry for <Share_Name>** dialog, set **Type** to *"All"* and **Applies to** to *"This folder, subfolder and files"*.

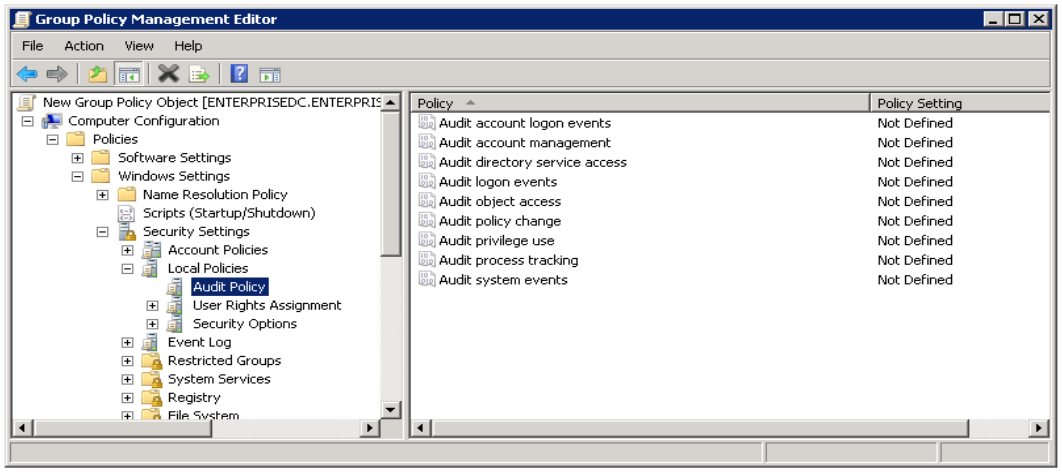
5. Click **Show advanced permissions** and select the following options:

   - To monitor successful read access and failed read access attempts:
     - List Folder / Read Data
   - To monitor successful modifications and failed modification attempts:
     - Create Files / Write Data
     - Create Folders / Append Data
     - Write Attributes
     - Write Extended Attributes
     - Delete Subfolders and Files
     - Delete
     - Change Permissions
     - Take Ownership

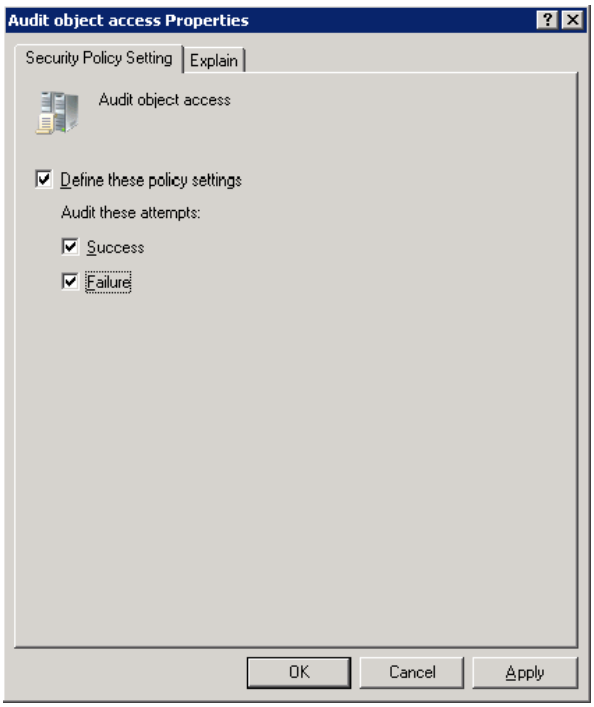
6. Make sure that the **Only apply these auditing settings to objects and/or containers within this container** check-box is cleared.

4.5.2. Configure Audit Object Access Policy

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains**, right-click **<domain_name>** and select **Create a GPO in this domain and Link it here**.
3. Enter the name for the new GPO.
4. Right-click the newly created GPO and select **Edit**.
5. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy.**



6. In the right pane, double-click **Audit object access** and select all check boxes in the **Audit object access Properties** dialog.



Refer to the Windows Server TechCenter article for additional information: Create a new Group Policy object: Group Policy. If you want to use a local policy, refer for instructions in the following Windows Server TechCenter article: Define or modify auditing policy settings for an event category: Auditing.

4.5.3. Configure Advanced Audit Policy

Configuring advanced audit will help you narrow the range of events monitored by the product, thus preventing your local Audit Archive and the Security Event Log from overfilling.

NOTE: The current version of Netwrix Auditor ignores the Advanced audit policy settings, as a result of which you will be getting warning messages if the audit policy subcategory configuration is applied.

These warning messages can be ignored, as they do not affect the product functionality. Netwrix plans to support Advanced auditing policies in the future product versions.

Perform one of the following procedures depending on the OS version:

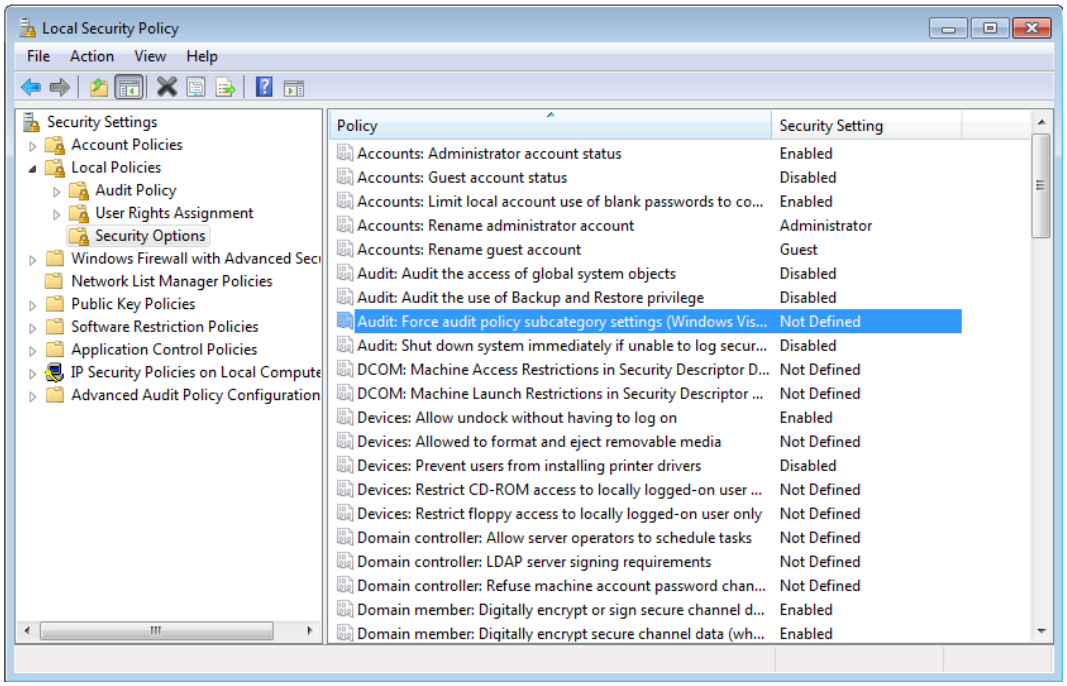
- To configure Advanced audit policy on Windows Server 2008 / Windows Vista
- To configure Advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

To configure Advanced audit policy on Windows Server 2008 / Windows Vista

In Windows Server 2008 / Windows Vista, audit policies are not integrated with the Group Policies and can only be deployed by using logon scripts generated with the native Windows **auditpol.exe** command line tool. Therefore, these settings are not permanent and will be lost after server reboot.

NOTE: The procedure below explains how to configure Advanced audit policy on a single file server. If you audit multiple file servers, you may want to create logon scripts and distribute them to all target machines via Group Policy. Refer to Microsoft Knowledge Base article: How to use Group Policy to configure detailed security auditing settings for more information.

1. On an audited file server, open the **Local Security Policy** snap-in: navigate to **Start** → **Run** and type *"secpol.msc"*.
2. Navigate to **Security Settings** → **Local Policies** → **Security Options** and locate the **Audit: Force audit policy subcategory settings (Windows Vista or later)** policy.



3. Double-click the policy to enable it.
4. Disable the **Object Access** category by executing the following command in the command line interface:

```
auditpol /set /category:"Object Access" /success:disable /failure:disable
```

5. Enable the following audit subcategories:

   - Handle Manipulation {0CCE9223-69AE-11D9-BED3-505054503030}.
   - File System {0CCE921D-69AE-11D9-BED3-505054503030}

   Execute the following commands in the command line interface:

   ```
   auditpol /set /subcategory:"File System" /success:enable /failure:enable
   ```

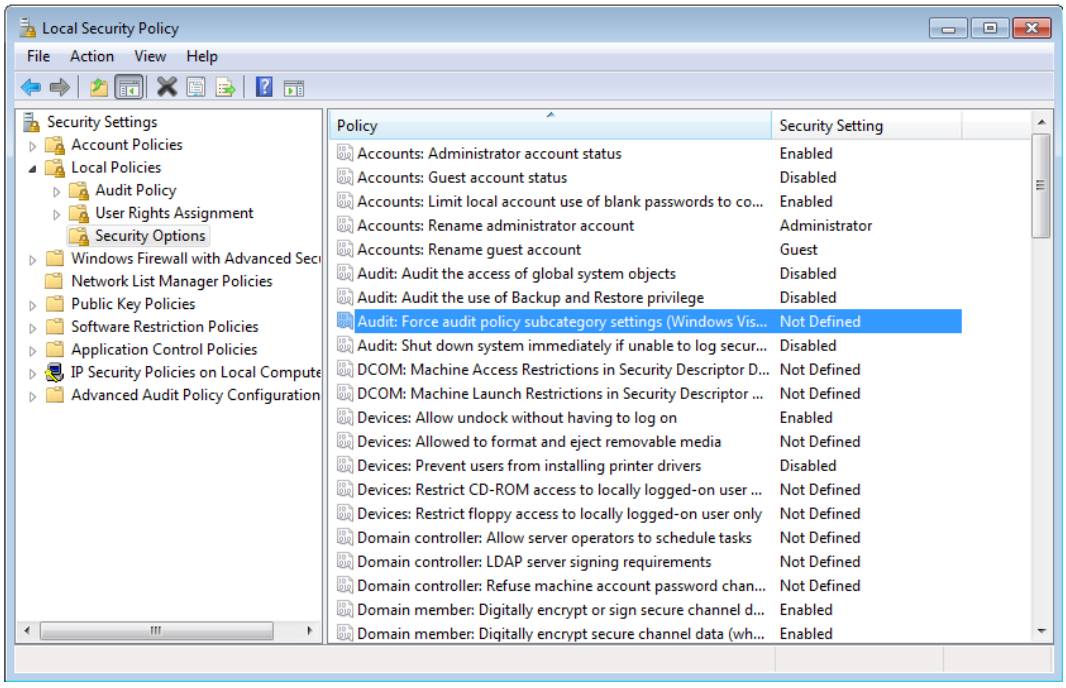
   ```
   auditpol /set /subcategoaury:"Handle Manipulation" /success:enable
   /failure:enable
   ```

   NOTE: It is recommended to disable all other subcategories unless you need them for other purposes. You can check your current effective settings by executing the following command: `auditpol /get /category:"Object Access"`.

To configure Advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

In Windows Server 2008 R2 and Windows 7 and above, Advanced audit policies are integrated with Group Policies, so they can be applied via Group Policy Object or Local Security Policies. The procedure below describes how to apply Advanced policies via Local Policies.

1. On an audited file server, open the **Local Security Policy** snap-in: navigate to **Start** → **Run** and type *"secpol.msc"*.
2. Navigate to **Security Settings** → **Local Policies** → **Security Options** and locate the **Audit: Force audit policy subcategory settings (Windows Vista or later)** policy.



3. Double-click the policy to enable it.

4. Navigate to **Security Settings** → **Advanced Audit Policy Configuration** → **System Audit Policies** → **Object Access** and enable the following subcategories:

   - Audit File System
   - Audit Handle Manipulation

   To do this, double click a subcategory, select **Configure the following audit events**. Select **Success** and/or **Failure** depending on the type of events you want to track.

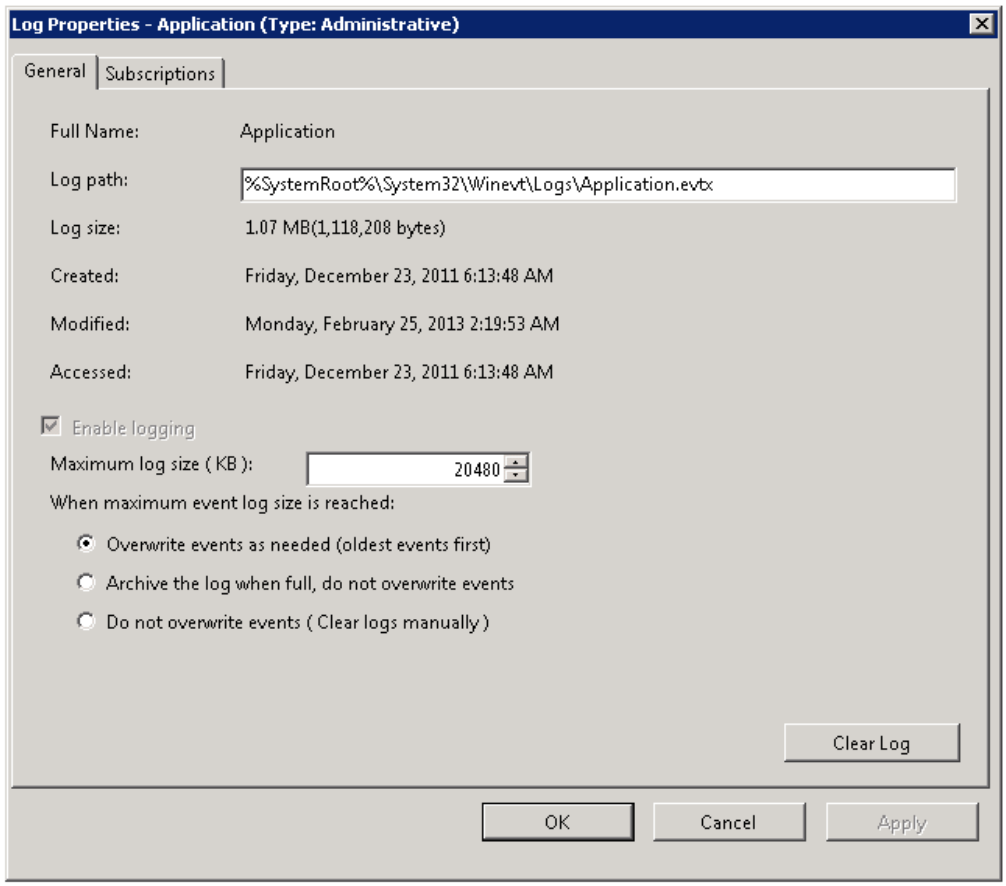
NOTE: You can check your current effective settings by executing the following command: `auditpol /get /category:"Object Access"`.

4.5.4. Configure Event Log Size and Retention Settings

The procedure below provides you with just one of a number of possible ways to adjust event log settings. If you have multiple target computers, you need to perform this procedure on each of them.

NOTE: If you move security log files from the default system folder to a non-default one, you must reboot your target server for the Reports functionality to work properly.

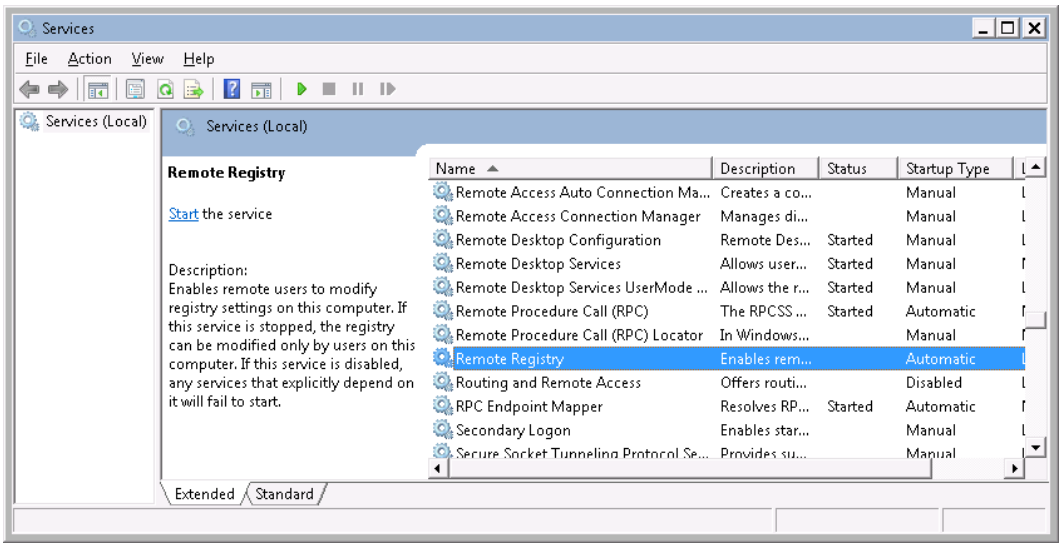
1. On a target server, navigate **Start** → **Programs** → **Administrative Tools** → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Windows Logs**, right-click **Application** and select **Properties**.



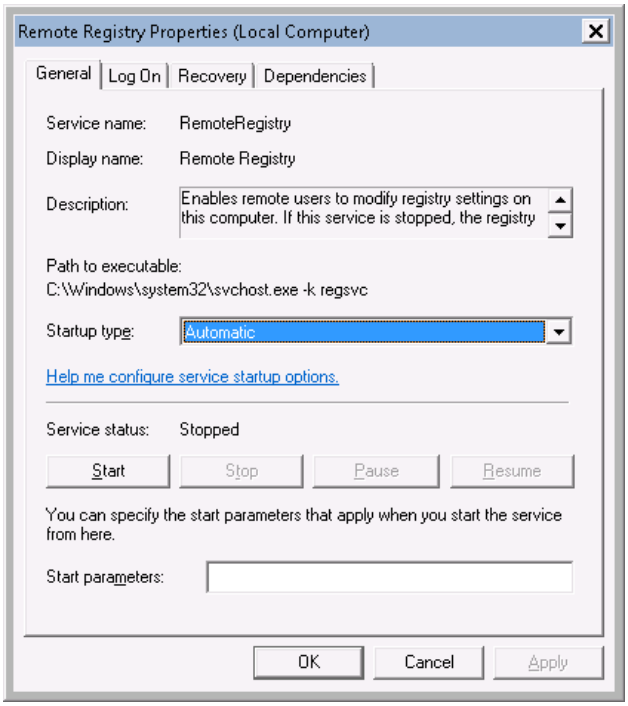
3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field specify the size:
   - On pre-Windows Vista versions—300MB
   - On Windows Vista and above—4GB
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If this option is selected, change the retention method by selecting another option: **Overwrite events as needed (oldest events first)**.

4.5.5. Enable Remote Registry Service

1. Navigate to **Start** → **Run** and type *"services.msc"*.



2. In the **Services** dialog locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) and the *"Running"* (on Windows Server 2012 and above) status.

4.6. Configure Infrastructure for NetApp Filer Auditing

The instructions in this section apply to the default VFiler. To audit several VFiler instances, you must perform these configuration steps for each of them.

NOTE: CIFS must be set up on your NetApp filer in advance.

The following commands are used:

- To get an option value:

  ```
  options <option_name>
  ```

- To set option value:

  ```
  options <option_name> <option_value>
  ```

To configure your infrastructure for NetApp Filer Auditing, perform the following procedures:

- Configure Qtree Security
- Configure Admin Web Access
- Configure Event Categories
- Configure Audit Settings for CIFS File Shares

4.6.1. Configure Qtree Security

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via the web interface (**FilerView** → **Filer** → **Use Command Line**).
2. Set the volume where the audited file shares are located to the *"ntfs"* security style:

```
apphost01> qtree status
Volume   Tree     Style Oplocks  Status
-------- -------- ----- -------- ---------
vol0              ntfs  enabled  normal
vol0     test     ntfs  enabled  normal
vol1              unix  enabled  normal
vol2              ntfs  enabled  normal
apphost01>
```

4.6.2. Configure Admin Web Access

Netwrix Auditor uses the NetApp API to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to an MS Event Viewer compatible format. Netwrix Auditor supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via the web interface (**FilerView** → **Filer** → **Use Command Line**).
2. Make sure that the `httpd.admin.enable` or `httpd.admin.ssl.enable` option is set to *"on"*. For security reasons, it is recommended to configure SSL access and enable the `httpd.admin.ssl.enable` option.

   If a non-default configuration is set for `httpd.admin.access` (i.e. *"limit access to trusted host only"* or *"allow admin web access for specific Ethernet interfaces"*), make sure that the Web Filer UI is accessible by the name of the audited file server. For example, the audit share `\\file_server\my_share\` must be viewed with the NetApp filer WebUI at `http(s)://file_server/na_admin/`.

```
apphost01> options httpd.admin
httpd.admin.access           legacy
httpd.admin.enable           off
httpd.admin.hostsequiv.enable off
httpd.admin.max_connections  512
httpd.admin.ssl.enable       on
httpd.admin.top-page.authentication on
apphost01>
```

4.6.3. Configure Event Categories

Perform the following procedures:

- Configure Audit Event Categories
- Configure Security Log
- Specify Security Log Shared Folder

4.6.3.1. Configure Audit Event Categories

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via the web interface (**FilerView** → **Filer** → **Use Command Line**).
2. Set the `cifs.audit.enable` and `cifs.audit.file_access_events.enable` options to *"on"*.
3. Unless you are going to audit logon events, set the `cifs.audit.logon_events.enable` and `cifs.audit.account_mgmt_events.enable` options to *"off"*.

   NOTE: It is recommended to turn off logon audting in order to reduce the number of events generated.

4.6.3.2. Configure Security Log

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via the web interface (**FilerView** → **Filer** → **Use Command Line**).
2. In order to avoid overwriting of the security logs, set the following values:
   - `cifs.audit.logsize 300 000 000 (300 MB)`
   - `cifs.audit.autosave.onsize.enable on`
   - `cifs.audit.autosave.file.extension timestamp`
3. Disable the `cifs.audit.liveview.enable` option since it interferes with the normal Security log behavior and prevents Netwrix Auditor from processing audit data properly.
4. To set up old logs deletion, you can configure the `cifs.audit.autosave.file.limit` option by specifying the maximum number of files to be stored, or enable the built-in automatic log deletion option in the Netwrix Auditor console.

Make sure there is enough disk space allotted to the security logs archives. Depending on the file access activity, audit data may grow rapidly, and the location specified for the security log (and security log auto archives) must be large enough to hold data until it is processed by Netwrix Auditor (by default, data collection runs every 24 hours). To set up old logs deletion, you can configure `the cifs.audit.autosave.file.limit` option by specifying the maximum number of files to be stored, or logs retention.

To configure logs retention period

1. On the computer where **Netwrix Auditor** is installed, open the Registry Editor: navigate to **Start**→ **Run** and type *"regedit"*.
2. Depending on your OS, navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Netwrix** → **File Server Change Reporter** (for 32-bit OS), or **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix** → **File Server Change Reporter** (for 64-bit OS).
3. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open.

   This value defines the time period (in hours) after which security event logs archives will be automatically deleted. By default, it is set to *"50"* (decimal). Modify this value, if necessary, and click **OK** to save the changes.

   NOTE: If the **CleanAutoBackupLogs** registry value is set to *"0"*, you will have to remove the old logs manually, or you may run out of space on your hard drive.

4.6.3.3. Specify Security Log Shared Folder

Netwrix Auditor accesses audit logs via a specified file share. This may be either the default administrative share (ETC$, C$, etc.), or a custom file share.

1. Navigate to the NetApp filer command prompt through the SSH/Telnet connection (depending on your NetApp filer settings), or via the web interface (**FilerView** → **Filer** → **Use Command Line**).
2. Use the `cifs shares` command to create a new file share or configure an existing share.

```
apphost01> cifs shares
Name          Mount Point                       Description
----          -----------                       -----------
ETC$          /etc                              Remote Administration
                        BUILTIN\Administrators / Full Control
C$            /                                 Remote Administration
                        BUILTIN\Administrators / Full Control
share1        /vol/vol0/shares/share1
                        everyone / Full Control
```

4.6.4. Configure Audit Settings for CIFS File Shares

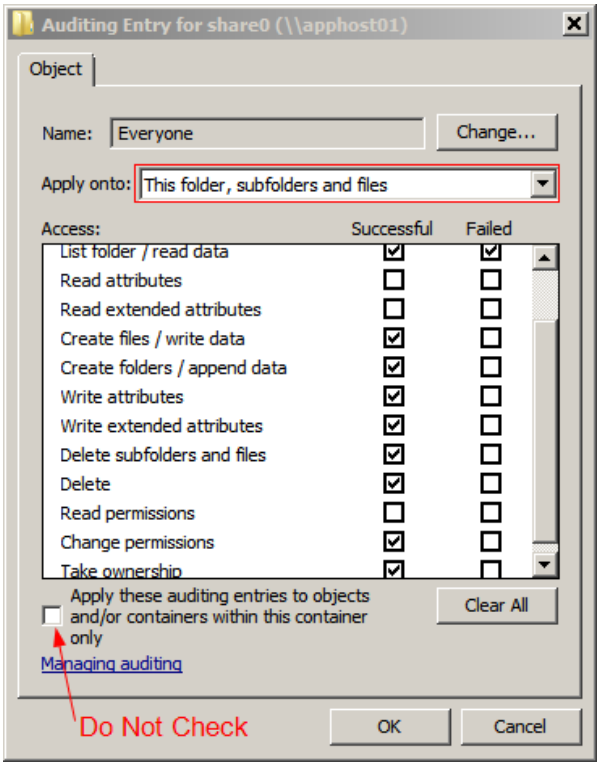
To configure audit settings for the CIFS file shares, perform the following steps on the audited file share:

1. Navigate to the root share folder, right-click it and select **Properties**.
2. Open the **Security** tab.

   NOTE: If there is no such tab, it means a wrong security style has been specified for the volume holding this file share. See Configure Qtree Security for more information.

3. Click **Advanced** and select the **Auditing** tab. Click **Edit**.

4. In the dialog that opens, select **Everyone**. Select **Successful** and **Failed** next to the following options:
   - Select **Successful** and **Failed** to monitor successful read access and failed read access attempts:
     - List Folder / Read Data
   - Select **Successful** to monitor successful modification attempts:
     - Create Files / Write Data
     - Create Folders / Append Data
     - Write Attributes
     - Write Extended Attributes
     - Delete Subfolders and Files
     - Delete
     - Change Permissions
     - Take Ownership
5. Make sure that **Apply these auditing entries to objects and/or containers within this container only** is cleared. Also, make sure that the **Apply onto** parameter is set to *"This folder, subfolders and files"*.



4.7. Configure Infrastructure for EMC Storage Auditing

To configure your infrastructure for EMC Storage Auditing, perform the following procedures:

- Configure Security Event Log Maximum Size to avoid overwriting of the security logs, it is recommended to set security log size to a maximum (4GB).

  By default, the security log is set to overwrite events that are older than 10 days, and its size is set to 512 KB. The default location for the security.evt log is **C:\security.evt**, which corresponds to the root partition of the Data Mover. To be able to increase the security log size, you must move it from the Data Mover root folder.

- Set the **Audit object access** policy set to *"Success"* and *"Failure"* in the Group Policy of the OU where your EMC VNX/VNXe/Celerra appliance belongs to. For more information on VNX/VNXe/Celerra GPO support, refer to documentation provided by EMC.

- Configure Audit Settings for CIFS File Shares on EMC VNX/ VNXe/ Celerra

4.7.1. Configure Security Event Log Maximum Size

1. On your file server, create a new file system where the security log will be stored.
2. Mount this file system on a mount point, e.g. **/events**.
3. Make sure that it is accessible via the **\\<file_server_name>\C$\events** UNC path.
4. On the computer where Netwrix Auditor is installed, open **Registry Editor:** navigate to **Start** → **Run** and type *"regedit"*.
5. Navigate to **File** → **Connect Network Registry** and specify the file server name.
6. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security** and set the **File** value to *"C:\events\security.evt"*.
7. Set the **MaxSize** value to *"4 000 000 000 (decimal)"*.

   NOTE: Due to Windows Server 2003 limitations, a security log larger than 300 MB cannot be processed.

8. Restart the corresponding Data Mover for the changes to take effect.

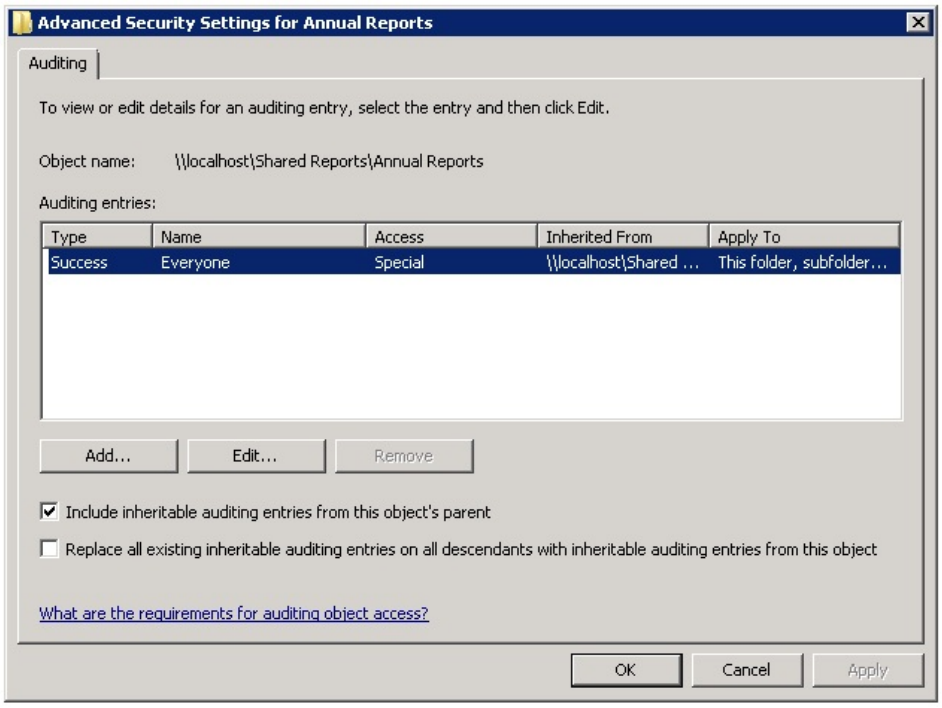
4.7.2. Configure Audit Settings for CIFS File Shares on EMC VNX/ VNXe/ Celerra

To configure audit settings for the CIFS file shares, perform the following procedure on the monitored file share:

1. Navigate to the target file share, right-click it and select **Properties**.
2. In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab, select **Everyone** (or another user-defined group containing users that are granted special permissions) and

click **Edit.**

4. In a separate **Advanced Security Settings for <Share_Name>** dialog, select **Everyone** and click **Edit**.

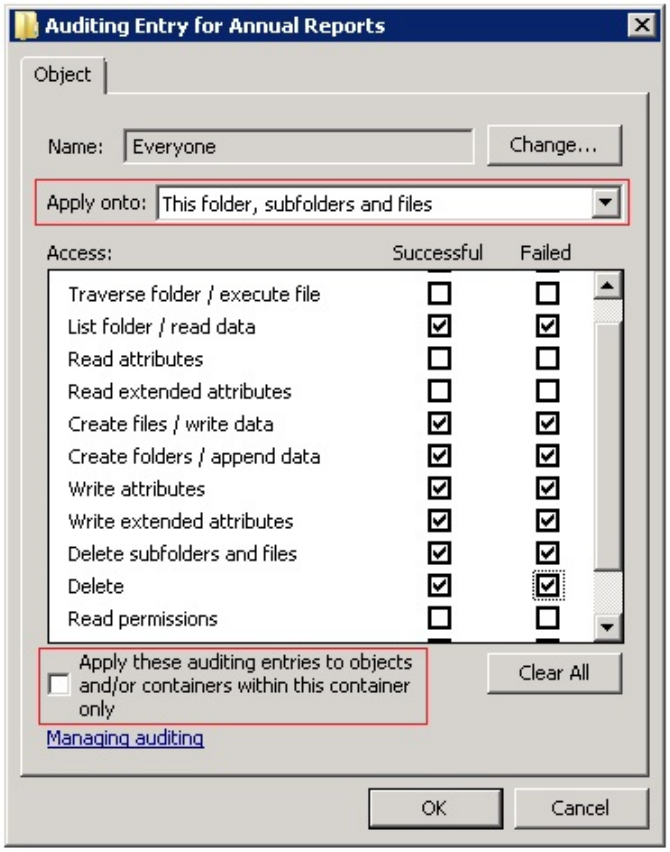


NOTE: You can specify any other user group, but in this case Netwrix Auditor will send emails with warnings on incorrect audit configuration. This will not affect the Reports functionality and the product will only monitor user accounts that belong to the selected group.

5. In the **Auditing Entry for <Share_Name>** dialog, select **Successful** and **Failed** next to the following options:

   - To monitor successful read access and failed read access attempts:
     - List Folder / Read Data
   - To monitor successful modifications and failed modification attempts:
     - Create Files / Write Data
     - Create Folders / Append Data
     - Write Attributes
     - Write Extended Attributes
     - Delete Subfolders and Files
     - Delete

- Change Permissions
- Take Ownership



6. Make sure that **Apply onto** is set to *"This folder, subfolders and files"*, and **Apply these auditing entries to objects and/or containers within this container only** is cleared.

4.8. Configure Infrastructure for Windows Server Auditing

You can configure your infrastructure for Windows Server Auditing in one of the following ways:

- Automatically when creating a Managed Object.

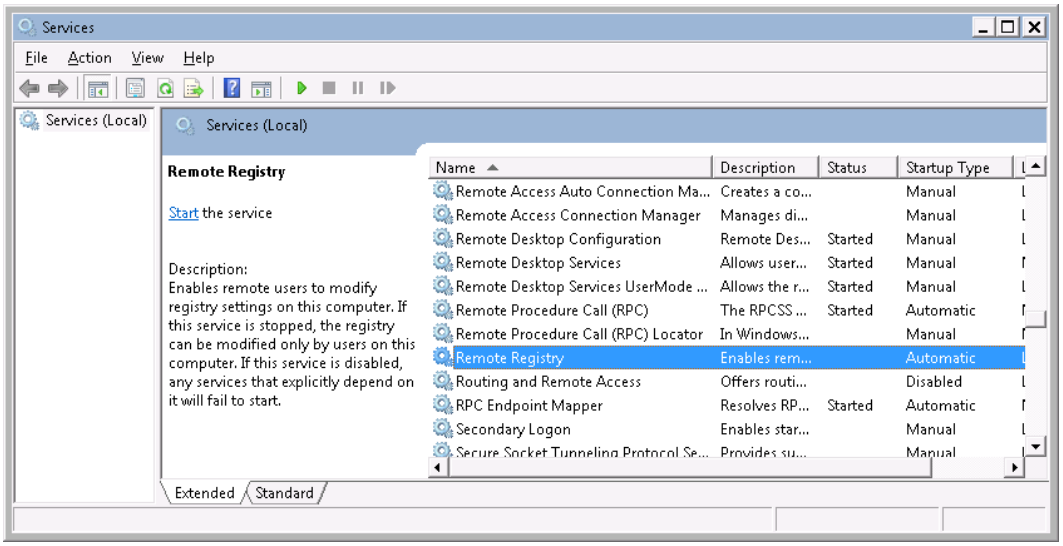
  If you select to configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary.

  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.

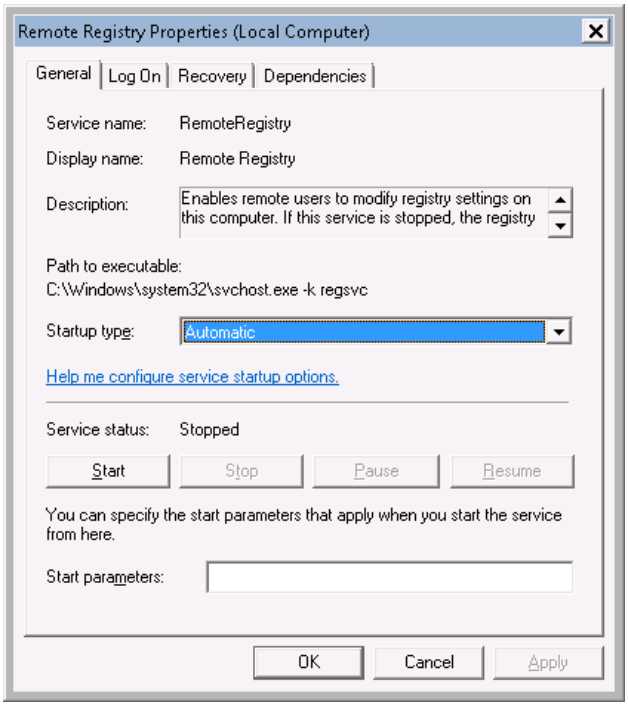
- Manually by performing the following procedures:
  - Enable Remote Registry and Windows Management Instrumentation Services
  - Configure Windows Registry Audit Settings
  - Configure Local Audit Policies
  - Configure Event Log Size and Retention Settings

4.8.1. Enable Remote Registry and Windows Management Instrumentation Services

1. Navigate to **Start** → **Run** and type *"services.msc"*.



2. In the **Services** dialog locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) and the *"Running"* (on Windows Server 2012 and above) status.
5. Locate the **Windows Management Instrumentation** service and repeat these steps.

4.8.2. Configure Windows Registry Audit Settings

Windows Registry audit permissions must be configured so that the "Who" and "When" values are reported correctly for each change. Configure these settings on each Windows server you want to audit.

The following audit permissions must be set to *"Successful"* for the `HKEY_LOCAL_MACHINE\SOFTWARE`, `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys:

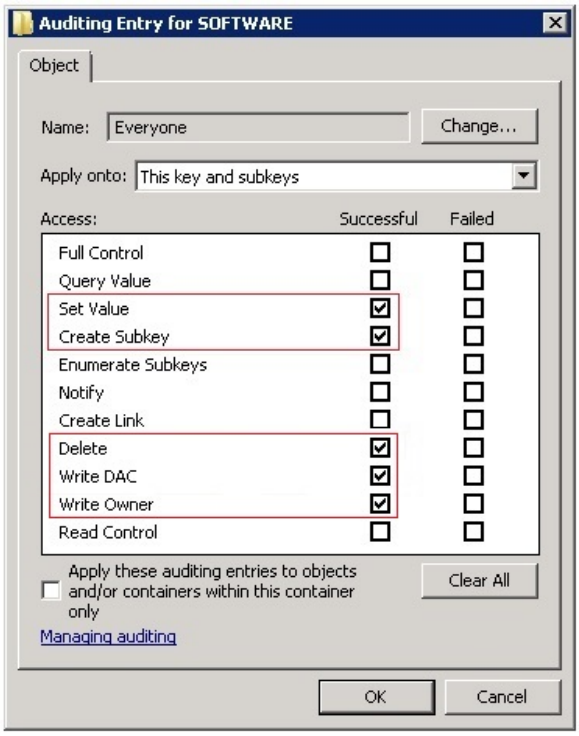
- Set Value
- Create Subkey
- Delete
- Write DAC
- Write Owner

Perform one of the following procedures depending on the OS version:

- To configure Windows registry audit settings on pre-Windows Server 2012 versions
- To configure Windows registry audit settings on Windows Server 2012 and above

To configure Windows registry audit settings on pre-Windows Server 2012 versions

1. On your target server, open **Registry Editor:** navigate to **Start** → **Run** and type *"regedit"*.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click **Advanced**.
4. In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.
5. Select the **Everyone** group.
6. In the **Auditing Entry for SOFTWARE** dialog, select *"Successful"* for the following access types: **Set Value**, **Create Subkey**, **Delete**, **Write DAC**, and **Write Owner.**

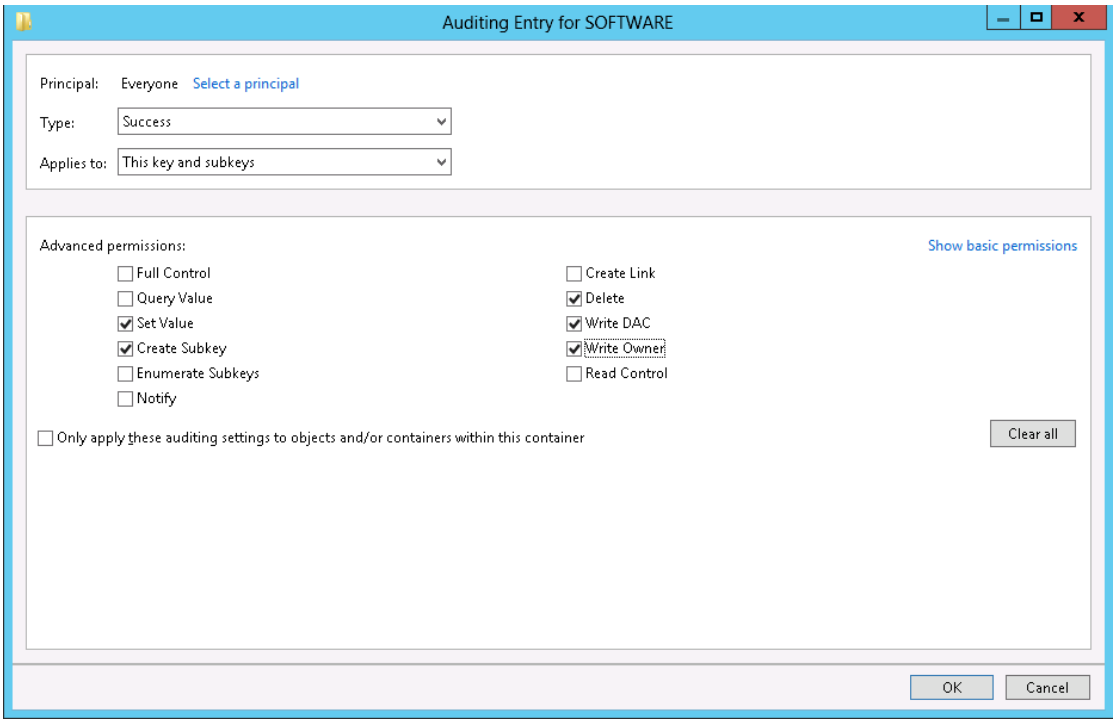


7. Repeat the same steps for the `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys.

To configure Windows registry audit settings on Windows Server 2012 and above

1. On your target server, open **Registry Editor:** navigate to **Start** → **Run** and type *"regedit"*.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click **Advanced**.
4. In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.
5. Click **Select a principal link** and specify the **Everyone** group in the **Enter the object name to select** field.
6. Set **Type** to *"Successful"* and **Applies to** to *"This key and subkeys"*.

7. Click **Show advanced permissions** and select the following access types: **Set Value**, **Create Subkey**, **Delete**, **Write DAC**, and **Write Owner**.



8. Repeat the same steps for the `HKEY_LOCAL_MACHINE\SYSTEM` and `HKEY_USERS\.DEFAULT` keys.

4.8.3. Configure Local Audit Policies

Local audit policies must be configured on the target servers to get the "Who" and "When" values for the changes to the following monitored system components:

- Services
- Hardware and system drivers
- Windows registry
- Scheduled tasks
- Local users and groups

NOTE: There are several methods to configure local audit policies, and this guide covers just one of them. Consider the possible impact on your environment and select the method that best suits your purposes. Note that if you follow the procedures below, audit settings will be applied to the whole domain.

Refer to the Windows Server TechCenter article for additional information: Create a new Group Policy object: Group Policy. If you want to use the local policy, refer to the following Windows Server TechCenter article: Define or modify auditing policy settings for an event category: Auditing.

Perform one of the following procedures depending on the OS version:

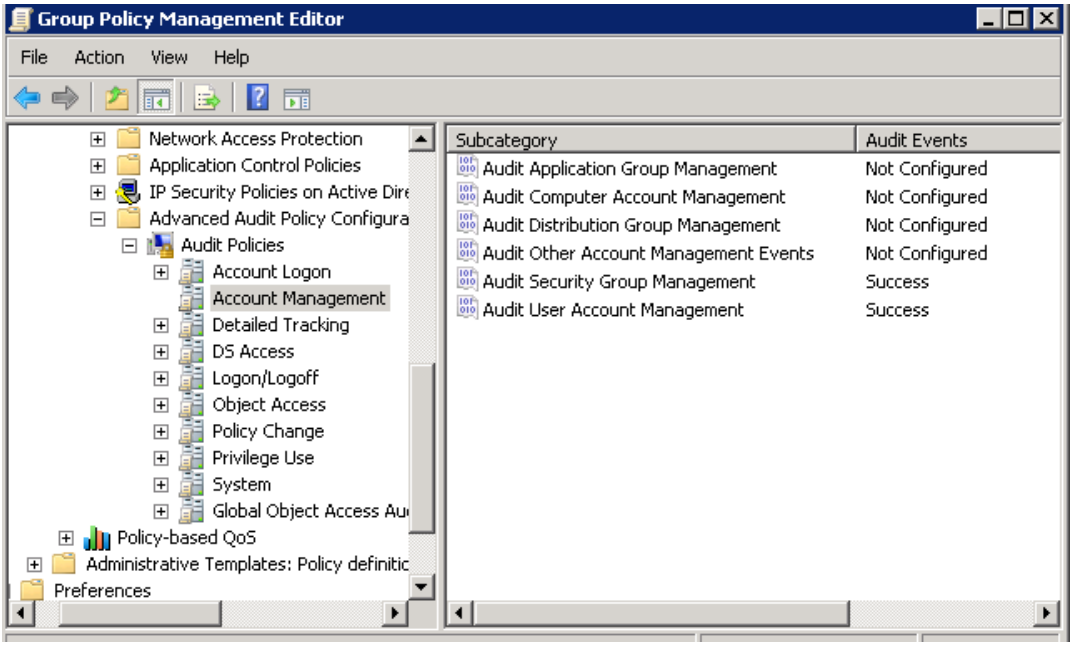
- To configure local audit policies on pre-Windows Vista versions
- To configure local audit policies on Windows Vista and above

To configure local audit policies on pre-Windows Vista versions

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains**, right-click **<domain_name>** and select **Create a GPO in this domain and Link it here**.
3. Enter the name for the new GPO.
4. Right-click the newly created GPO and select **Edit**.
5. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy.**
6. Double-click **Audit account management** on the right, select **Success** in the properties dialog.
7. Double-click **Audit object access** on the right, select **Success** in the properties dialog.
8. Navigate to **Start** → **Run** and type *'"cmd"*. Input the `gpupdate /force` command and click **Enter**. The group policy will be updated.

To configure local audit policies on Windows Vista and above

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains**, right-click **<domain_name>** and select **Create a GPO in this domain and Link it here**.
3. Enter the name for the new GPO.
4. Right-click the newly created GPO and select **Edit**.
5. In the Group Policy Management Editor dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policies** → **Account Management.**



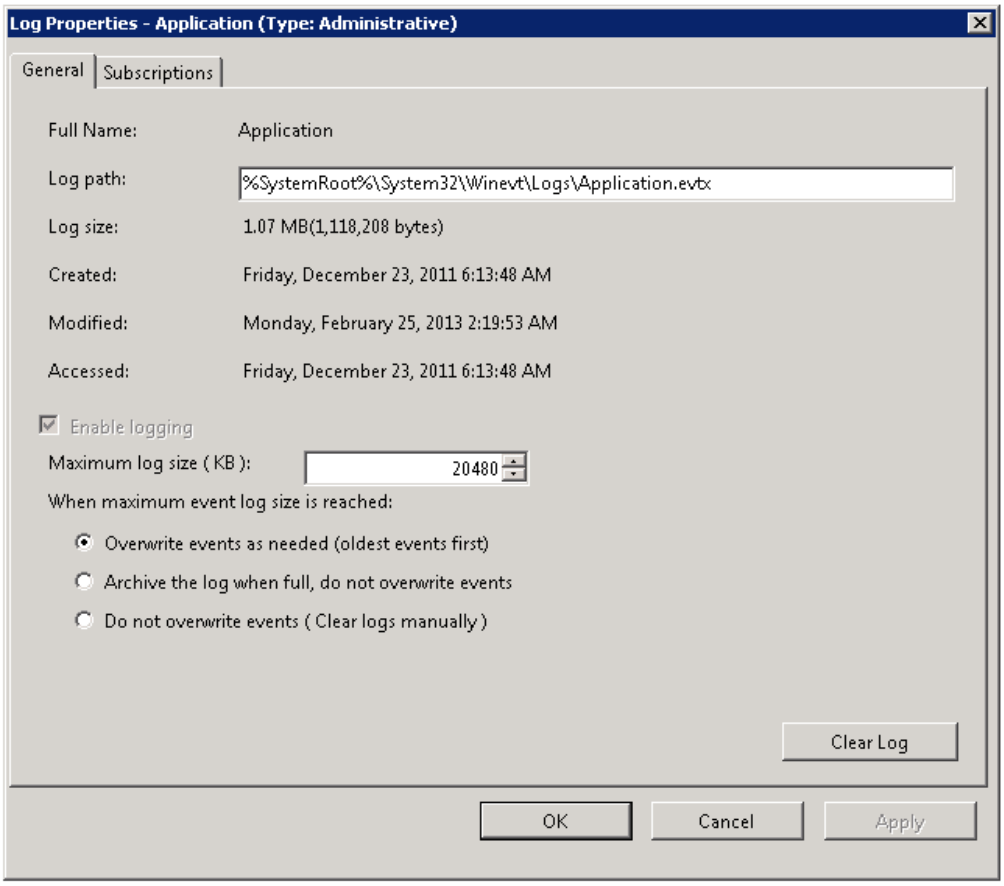
6. Double-click **Audit Security Group Management** on the right, select **Success** in the properties dialog.
7. Double-click **Audit User Account Management** on the right, select **Success** in the properties dialog.
8. Locate **Object Access** under the **Audit Policies** node.
9. Double-click **Audit Handle Manipulation** on the right, select **Success** in the properties dialog.
10. Repeat the previous step for the **Audit Other Object Access Events** and **Audit Registry** policies.
11. Navigate to **Start** → **Run** and type *'"cmd"*. Input the `gpupdate /force` command and click **Enter**. The group policy will be updated.

4.8.4. Configure Event Log Size and Retention Settings

To prevent data loss, you need to specify the maximum size for the Application, Security, System and Microsoft-Windows-TaskScheduler/ Operational event logs. The procedure below provides you with just one of a number of possible ways to specify the event log settings. If you have multiple target computers, you need to perform this procedure on each of them.

To configure the event log size and retention method

1. On a target server, navigate **Start** → **Programs** → **Administrative Tools** → **Event Viewer**.
2. Navigate to **Event Viewer tree** → **Windows Logs**, right-click **Application** and select **Properties**.



3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field specify the size:
   - On pre-Windows Vista versions—300MB
   - On Windows Vista and above—4GB
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If this option is selected, change the retention method by selecting another option: **Overwrite events as needed (oldest events first)**.
6. Repeat these steps for the **Security** and **System** event logs under **Windows Logs**, and for **Microsoft-Windows-TaskScheduler/Operational** event log by navigating to **Applications and Services Logs** → **Microsoft** → **Windows** → **TaskScheduler** → **Operational**.

4.9. Configure Infrastructure for Event Log Management

Do one of the following: depending on the OS:

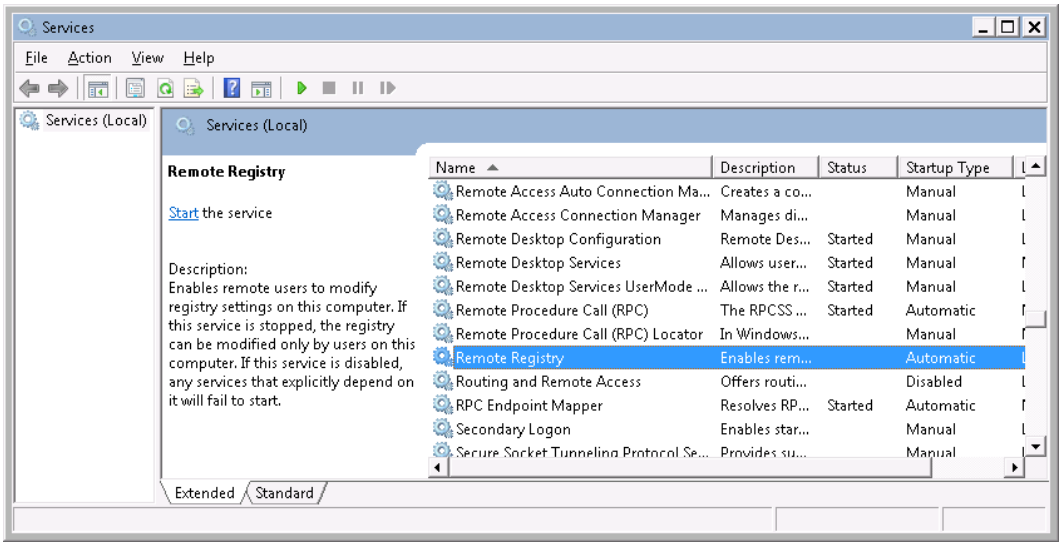
- Configure Event Log Management on Windows Computers
- Configure Event Log Management on Syslog-Based Platforms

4.9.1. Configure Event Log Management on Windows Computers

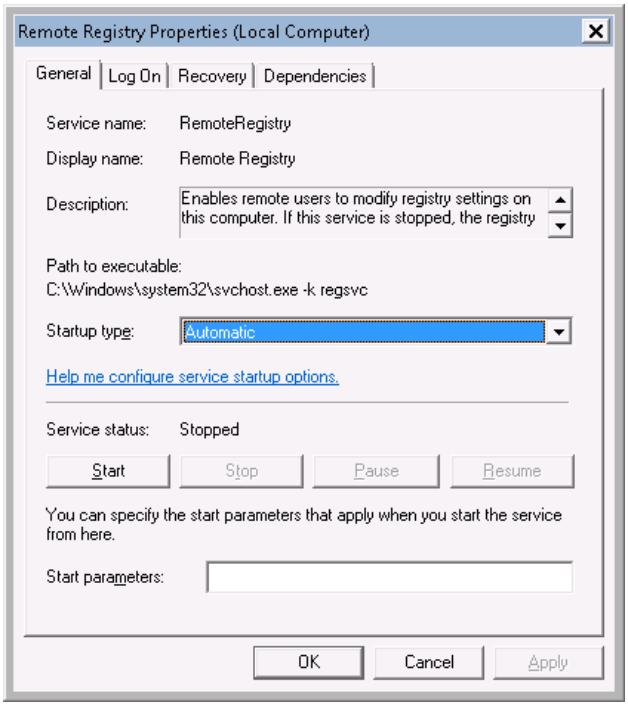
The **Remote Registry** service must be enabled on the target computers.

NOTE: You only need to perform this procedure if you choose to use the agentless data collection method.

1. Navigate to **Start** → **Run** and type *"services.msc"*.



2. In the **Services** dialog locate the **Remote Registry** service, right-click it and select **Properties**.
3. In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



4. In the **Services** dialog, ensure that **Remote Registry** has the *"Started"* (on pre-Windows Server 2012 versions) and the *"Running"* (on Windows Server 2012 and above) status.

4.9.2. Configure Event Log Management on Syslog-Based Platforms

To be able to process Syslog events, you must configure the Syslog daemon to redirect these events to the computer where Netwrix Auditor is installed.

The procedure below explains how to configure redirection of **Auth log**, as predefined Syslog-based platforms in Netwrix Auditor have default rules to process this log only. You can create your own rules and configure syslog platform settings as described in the procedure below. Refer to Netwrix Auditor Administrator's Guide for more information.

To configure a Syslog daemon to redirect events for Red Hat Enterprise Linux 5

1. Open the **/etc/syslog.conf** file.
2. Add the following line: `authpriv.* @FQDN/Netbios name` or `authpriv.* @ComputerIP`.

   NOTE: `FQDN/Netbios name` and `ComputerIP` must be the name and IP address of the computer where Netwrix Auditor is installed.
3. Navigate to the **/etc/sysconfig/syslog** file.
4. Change the **SYSLOGD_OPTIONS** value to *SYSLOGD_OPTIONS="-r –m 0"*.
5. Launch the **RHEL** console and execute the following command: `service syslog restart`.

To configure a Syslog daemon to redirect events for Ubuntu 11

1. Navigate to the **/etc/rsyslog.d/50-default.conf** file.
2. Add the following line: `authpriv.* @FQDN/Netbios name` or `authpriv.* @ComputerIP`

   NOTE: `FQDN/Netbios name` and `ComputerIP` must be the name and IP address of the computer where Netwrix Auditor is installed.
3. Launch the **UBUNTU** console and execute the following command: `service rsyslog restart`.

4.10. Configure Computers for User Activity Video Recording

For instructions on how to configure your infrastructure for User Activity Video Recording, refer to the following sections:

- Configure Data Collection Settings
- Configure Video Recordings Playback Settings

4.10.1. Configure Data Collection Settings

To successfully track user activity, make sure that the following settings are configured on the monitored computers and on the computer where Netwrix Auditor is installed:

- The **Windows Management Instrumentation** and the **Remote Registry** services are running and their **Startup Type** is set to *"Automatic"*. See To check the status and startup type of Windows services for more information.
- The **File and Printer Sharing** and the **Windows Management Instrumentation** features are allowed to communicate through Windows Firewall. See To allow Windows features to communicate through Firewall for more information.
- Local TCP Port 9002 is opened for inbound connections on the computer where Netwrix Auditor is installed. See To open Local TCP Port 9002 for inbound connections for more information.
- Local TCP Port 9003 is opened for inbound connections on the monitored computers. See To open Local TCP Port 9003 for inbound connections for more information.
- Remote TCP Port 9002 is opened for outbound connections on the monitored computers. See To open Remote TCP Port 9002 for outbound connections for more information.

To check the status and startup type of Windows services

1. Navigate to **Start** → **Run** and type *"services.msc"*.
2. In the **Services** snap-in, locate the **Remote Registry** service and make sure that its status is *"Started"*

(on pre-Windows Server 2012 versions) and *"Running"* (on Windows Server 2012 and above). If it is not, right-click the service and select **Start** from the pop-up menu.

3. Check that the **Startup Type** is set to *"Automatic"*. If it is not, double-click the service. In the **Remote Registry Properties** dialog, in the **General** tab, select *"Automatic"* from the drop-down list.
4. Perform the steps above for the **Windows Management Instrumentation** service.

To allow Windows features to communicate through Firewall

1. Navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Allow a program or feature through Windows Firewall** on the left.
3. In the **Allow programs to communicate through Windows Firewall** page that opens, locate the **File and Printer Sharing** feature and make sure that the corresponding check-box is selected under **Domain**.
4. Repeat step 3 for the **Windows Management Instrumentation (WMI)** feature.

To open Local TCP Port 9002 for inbound connections

1. On computer where Netwrix Auditor is installed, navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.
4. Click **New Rule**. In the **New Inbound Rule** wizard, complete the steps as described below:
   - On the **Rule Type** step, select **Program**.
   - On the **Program** step, specify the path: *%Netwrix Auditor installation folder%/Netwrix/User Activity Video Recorder/UAVRServer.exe*.
   - On the **Action** step, select the **Allow the connection** action.
   - On the **Profile** step, make sure that the rule applies to **Domain**.
   - On the **Name** step, specify the rule's name, for example **UAVR Server inbound rule**.
5. Double-click the newly created rule and open the **Protocols and Ports** tab.
6. In the **Protocols and Ports** tab, complete the steps as described below:
   - Set **Protocol** type to *"TCP"*.
   - Set **Local port** to *"Specific Ports"* and specify to *"9002"*.

To open Local TCP Port 9003 for inbound connections

1. On a target computer navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.
4. Click **New Rule**. In the **New Inbound Rule** wizard, complete the steps as described below:
   - On the **Rule Type** step, select **Program**.
   - On the **Program** step, specify the path to the agent: *%Netwrix%/User Activity Video Recorder Agent/UAVRAgent.exe*.
   - On the **Action** step, select the **Allow the connection** action.
   - On the **Profile** step, make sure that the rule applies to **Domain**.
   - On the **Name** step, specify the rule's name, for example **UAVR Agent inbound rule**.
5. Double-click the newly created rule and open the **Protocols and Ports** tab.
6. In the **Protocols and Ports** tab, complete the steps as described below:
   - Set **Protocol** type to *"TCP"*.
   - Set **Local port** to *"Specific Ports"* and specify to *"9003"*.

To open Remote TCP Port 9002 for outbound connections

1. On a target computer, navigate to **Start** → **Control Panel** and select **Windows Firewall.**
2. In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.
3. In the **Windows Firewall with Advanced Security** dialog, select **Inbound Rules** on the left.
4. Click **New Rule**In the **New Inbound Rule** wizard, complete the steps as described below:
   - On the **Rule Type** step, select **Program**.
   - On the **Program** step, specify the path to the agent: *%Netwrix%/User Activity Video Recorder Agent/UAVRAgent.exe*.
   - On the **Action** step, select the **Allow the connection** action.
   - On the **Profile** step, make sure that the rule applies to **Domain**.
   - On the **Name** step, specify the rule's name, for example **UAVR Agent outbound rule**.
5. Double-click the newly created rule and open the **Protocols and Ports** tab.
6. In the **Protocols and Ports** tab, complete the steps as described below:

- Set **Protocol** type to *"TCP"*.
- Set **Remote port** to *"Specific Ports"* and specify to *"9002"*.

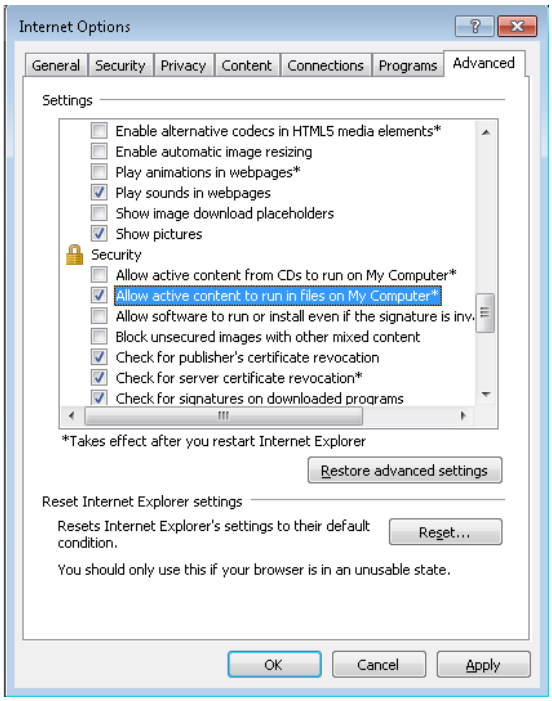
4.10.2. Configure Video Recordings Playback Settings

Video recordings of users' activity can be watched in the Netwrix Auditor console. They are also available as links in web-based reports and attachments in the emails with Activity Summaries and subscriptions. To be able to watch video files captured by Netwrix Auditor, the following settings must be configured:

- Microsoft Internet Explorer 6.0 or above must be installed and ActiveX must be enabled.
- Internet Explorer security settings must be configured properly. See To configure Internet Explorer security settings for more information.
- JavaScript must be enabled. See To enable JavaScript for more information.
- Internet Explorer Enhanced Security Configuration (IE ESC) must be disabled. See To disable Internet Explorer Enhanced Security Configuration (IE ESC) for more information.
- The user must belong to the **Netwrix User Activity Video Reporter Auditors** group that has access to the **Netwrix_UAVR$** shared folder where video files are stored. Both the group and the folder are created automatically by Netwrix Auditor. See To add users to the Netwrix User Activity Video Reporter Auditors group for more information.
- A dedicated codec must be installed. This codec is installed automatically on the computer where Netwrix Auditor is deployed, and on the monitored computers. To install it on a different computer, download it from http:/www.Netwrix.com/download/ScreenPressorNetwrix.zip.

To configure Internet Explorer security settings

1. In **Internet Explorer**, navigate to **Tools** → **Internet Options**.
2. Switch to the **Security** tab and select **Local Intranet**. Click **Custom Level**.
3. In the **Security Settings – Local Intranet Zone** dialog, scroll down to **Downloads**, and make sure **File download** is set to *"Enable"*.
4. In the **Internet Options** dialog switch to the **Advanced** tab.
5. Scroll down to **Security** and make sure **Allow active content to run in files on My Computer** is selected.



To enable JavaScript

1. In **Internet Explorer**, navigate to **Tools** → **Internet Options**.
2. Switch to the **Security** tab and select **Internet**. Click **Custom Level**.
3. In the **Security Settings – Internet Zone** dialog, scroll down to **Scripting** and make sure **Active scripting** is set to *"Enable"*.

To disable Internet Explorer Enhanced Security Configuration (IE ESC)

1. Navigate to **Start** → **Administrative Tools** → **Server Manager**.
2. In the **Security Information** section, click the **Configure IE ESC** link on the right and turn it off.

To add users to the Netwrix User Activity Video Reporter Auditors group

Depending on the computer type (workstation or domain controller) where Netwrix Auditor is installed, do one of the the following:

- If Netwrix Auditor is installed on a workstation:
    1. Navigate to **Start** → **Control Panel** → **Administrative Tools** → **Computer Management**.
    2. In the **Computer Management** dialog, in the left pane, navigate to **System Tools** → **Local Users and Groups** → **Groups**.
    3. In the right pane, right-click **Netwrix User Activity Video Reporter Auditors**, and select **Properties**. Click **Add** and specify the users that you want to add to this group.

- If Netwrix Auditor is installed on a domain controller:
  1. Navigate to **Start** → **Administrative Tools** → **Active Directory Users and Computers**.
  2. Navigate to **<your_domain_name>** → **Users**.
  3. In the right pane, right-click **Netwrix User Activity Video Reporter Auditors**, and select **Properties**.
  4. In the dialog that opens, select the **Members** tab. Click **Add** and specify the users that you want to add to this group.

4.11. Configure Farm for SharePoint Auditing

You can configure your SharePoint farm for auditing in one of the following ways:

- Automatically when creating a Managed Object. If you select to configure audit in the target SharePoint farm automatically, your current audit settings will be checked on each data collection and adjusted if necessary.
- Manually by performing the following procedures:
  - Configure Audit Log Trimming on your SharePoint farm.
  - Configure Events Auditing Settings on your SharePoint farm.
  - Enable NetTcpPortSharing Service on the computer where Netwrix Auditor is installed.
  - Enable SPAdminV4 Service on the computer where SharePoint Central Administration is installed and where you intend to deploy Netwrix Auditor Agent for SharePoint.

4.11.1. Configure Audit Log Trimming

1. Log in as an administrator to the audited SharePoint site collection.
2. At the top level of your site collection navigate to **Settings** → **Site Settings**.
3. Select **Site collection audit settings** under **Site Collection Administration**.
4. In the **Audit Log Trimming** section, do the following:
   - Set **Automatically trim the audit log for this site** to *"Yes"*.
   - In **Specify the number of days of audit log data to retain** set retention to 7 days.

     NOTE: You may keep the existing audit log retention provided that it is set to 7 days or less.

4.11.2. Configure Events Auditing Settings

1. Log in as an administrator to the audited SharePoint site collection.
2. At the top level of your site collection navigate to **Settings** → **Site Settings**.

3. Select **Site collection audit settings** under **Site Collection Administration**.
4. In the **List, Libraries, and Sites** section select **Editing users and permissions**.

4.11.3. Enable NetTcpPortSharing Service

1. On the computer where Netwrix Auditor is installed, open the **Services Management Console**. Navigate to **Start** → **Run** and type *"services.msc"*.
2. Locate the **Net. Tcp Port Sharing** service (NetTcpPortSharing), right-click it and select **Properties**.
3. On the **General** tab, set **Startup type** to *"Manual"* and click **Apply**.
4. Click **Start** to start the service.

4.11.4. Enable SPAdminV4 Service

This service is must be started to ensure the Netwrix Auditor Agent for SharePoint successful installation. Perform the procedure below, prior to the agent installtion. See Install Netwrix Auditor Agent for SharePoint for more information.

1. On the computer where SharePoint Central Administration is installed and where you intend to deploy Netwrix Auditor Agent for SharePoint, open the **Services Management Console**. Navigate to **Start** → **Run** and type *"services.msc"*.
2. Locate the **SharePoint Administration** service (SPAdminV4), right-click it and select **Properties**.
3. On the **General** tab, set **Startup type** to *"Automatic"* and click **Apply**.
4. Click **Start** to start the service.

5. Configure Data Processing Account Rights and Permissions

The Data Processing Account is specified on Managed Object creation and is used by Netwrix Auditor to collect audit data from the target systems and applications.

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

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

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

Feature	Rights and Permissions
Active Directory Auditing	• Member of the **domain Administrators** group / the **Manage auditing and security log** policy must be defined for this account • The **Log on as a batch job** policy must be defined for this account • A member of the **local Administrators** group on the computer where the product is installed • The **Read** rights to the Active Directory **Deleted Objects** container • If event logs autobackup is enabled: permissions to the following registry key on each domain controller in the target domain: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* AND member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators** • If event logs autobackup is enabled: the **Share Read** and **Write** permissions and **Security Full control** permissions for the logs backup folder • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • The **Content Manager** role on the SSRS Home folder
Group Policy Auditing	• A member of the **domain Administrators** group / **Manage auditing and security log** policy defined for this account

Feature	Rights and Permissions
	• The **Log on as a batch job** policy defined for this account • The **Read** rights to the **Deleted Objects** AD container • If event logs autobackup is enabled: permissions to the following registry key on each domain controller in the target domain: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* AND the member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators** • The **Share Read** and **Write** permissions and **Security Full control** permissions for the logs backup folder (if auto backups are configured) • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • The **Content Manager** role on the SSRS Home folder
Exchange Server Auditing	• A member of the **domain Administrators** group / The **Manage auditing and security log** policy defined for this account • The **Log on as a batch job** policy defined for this account • The account must belong to **Organization Management** or **Records Management** group / **Audit Logs management** role must be assigned to this account (only required if the monitored AD domain has an Exchange organization running MS Exchange Server 2010 or 2013). • The **Read** rights to the **Deleted Objects** AD container • If event logs autobackup is enabled: permissions to the following registry key on each DC in the target domain: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* AND the member of one of the following groups: **Administrators**, **Print Operators**, **Server Operators** • **Share Read** and **Write** permissions and **Security Full control** permissions for the logs backup folder (if auto backups are configured) • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • The **Content Manager** role on the SSRS Home folder

Feature	Rights and Permissions
Mailbox Access Auditing	• A member of the **domain Administrators** group (to monitor several Exchange Servers in the domain where Netwrix Auditor is installed) / Member of **enterprise Administrators** group (to audit Exchange Servers in different domains belonging to the same forest)
Windows File Server Auditing	• A member of the **local Administrators** group If the computer where the product is installed and the audited servers belong to different domains, the target computers must have accounts with the same name and password as the Data Processing Account. All these account must be assigned the local administrator permissions. • The **Log on as a batch job** policy must be defined for this account • The **Manage auditing and security log** policy must be defined for this account • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • **Read access** to the monitored shared folders • The **Content Manager** role on the SSRS Home folder
EMC Storage Auditing	• A member of the **local Administrators** group If the computer where the product is installed and monitored servers belong to different domains, the target computers must have accounts with the same name and password as the Data Processing Account. All these account must be assigned the local administrator permissions. • The **Log on as a batch job** policy defined for this account • The **Manage auditing and security log** policy defined for this account • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • **Read access** to the monitored shared folders • The **Content Manager** role on the SSRS Home folder
NetApp Filer Auditing	• A member of the **local Administrators** group If the computer where the product is installed and monitored servers belong to different domains, the target computers must have accounts with the same name and password as the Data Processing Account. All these account must be assigned the local administrator permissions.

Feature	Rights and Permissions

	• The **Log on as a batch job** policy must be defined for this account
	• The **Manage auditing and security log** policy must be defined for this account
	• The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data)
	• **Read access** to the monitored shared folders
	• NetApp Filer account should have the following capabilities:
	  ◦ **login-http-admin**
	  ◦ **api-system-cli**
	  ◦ **api-options-get**
	  ◦ **cli-cifs**
	• The **Content Manager** role on the SSRS Home folder

Windows Server Auditing	• A member of the **local Administrators** group If the computer where the product is installed and monitored servers belong to different domains, the target computers must have accounts with the same name and password as the Data Processing Account. All these accounts must be assigned the local administrator permissions. • The **Log on as a batch job** policy defined for this account • The **Manage auditing and security log** policy must be defined for this account • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • The **Content Manager** role on the SSRS Home folder
SQL Server Auditing	• A member of the **local Administrators** group • The **System Administrator** role on the target SQL Server • The **Log on as a batch job** policy defined for this account • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data)
VMware Auditing	• A member of the **local Administrators** group • At least **Read-only**role on the monitored server(s)

Feature	Rights and Permissions
	• The **Log on as a batch job** policy defined for this account • The **Database owner** role assigned to account that is going to access the SQL database with audit data • The **Content Manager** role on the SSRS Home folder
Password Expiration Alerting	• A member of the **domain Administrators** group • The **Log on as a batch job** policy must be defined for this account
Inactive User Tracking	• A member of the **domain Administrators** group • The **Log on as a batch job** policy must be defined for this account
Event Log Management	• A member of the **domain Administrators** group • The **Log on as a batch job** policy must be defined for this account • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • The **Content Manager** role on the SSRS Home folder
User Activity Video Recording	• A member of the **local Administrators** group • The **Write** permissions for the product logs and the Audit Archive folder • The **Log on as a batch job** policy defined for this account • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • The **Content Manager** role on the SSRS Home folder
SharePoint Auditing	Required for Netwrix Auditor to function properly: • A member of the **local Administrators** group • A member of the **Domain Users** group • The **Log on as a service** policy must be defined for this account • The **Database owner** role must be assigned to this account if it going to access the SQL database with audit data) • The **Content Manager** role on the SSRS Home folder Required for the automatic installation of Netwrix Auditor Agent for SharePoint: • A member of the **local Administrators** group on SharePoint server, where

Feature	Rights and Permissions
	the agent will be deployed • The **SharePoint_ Shell_ Access** role on the SharePoint SQL Server configuration database

Follow the procedures below to configure Data Processing Account account rights and permissions:

- Configure Manage Auditing And Security Log Policy
- Define Log On As A Batch Job Policy
- Define Log On As A Service Policy
- Assign Database Owner (dbo) Role
- Assign System Administrator Role
- Grant Permissions for AD Deleted Objects Container
- Assign Permissions To Registry Key
- Add Account to Organization Management Group
- Assign Audit Logs Role To Account
- Assign Content Manager Role To Account
- Assign SharePoint_Shell_Access Role

5.1. Configure Manage Auditing And Security Log Policy

NOTE: You only need to perform this procedure if the Data Processing Account does not belong to the **domain Administrators** group.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains** → **<domain_name>** → **Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies.**
4. On the right, double-click the **User Rights Assignment** policy.
5. Locate the **Manage auditing and security log** policy and double-click it.

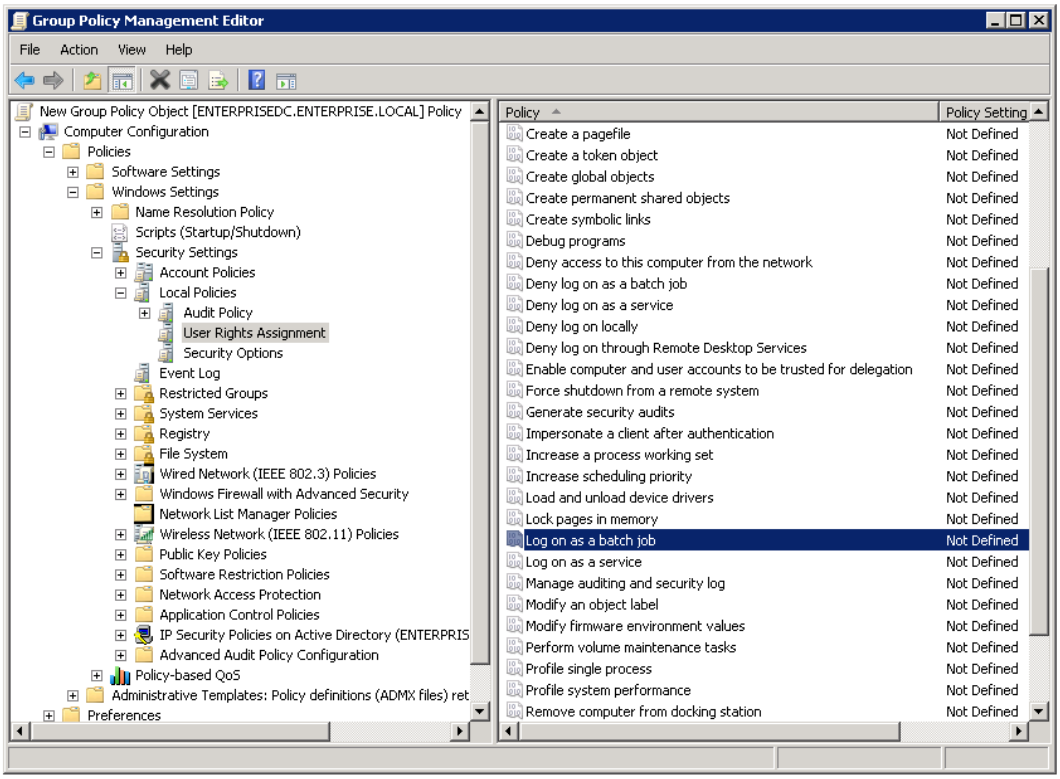
6. In the **Manage auditing and security log Properties** dialog, click **Add User or Group**, specify the user that you want to define this policy for.
7. Navigate to **Start** → **Run** and type *'"cmd"*. Input the `gpupdate /force` command and click **Enter**. The group policy will be updated.

5.2. Define Log On As A Batch Job Policy

On Managed Object creation, the **Log on as a batch job** policy is automatically defined for the Data Processing Account as a local security policy. However, 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 be reset. In this case, you need to redefine the policy on the domain level through the **Group Policy Management** console.

NOTE: You must define the **Log on as a batch job** policy for the Data Processing Account used for NetApp Filer Auditing and EMC Storage Auditing manually.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains** → **<domain_name>**, right-click **Default Domain Policy** and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **User Rights Assignment** and locate the **Log on as a batch job** policy.



4. Double-click the **Log on as a batch job** policy, select **Define these policy settings** and click **Add User or Group**. Specify the account that you want to define this policy for.

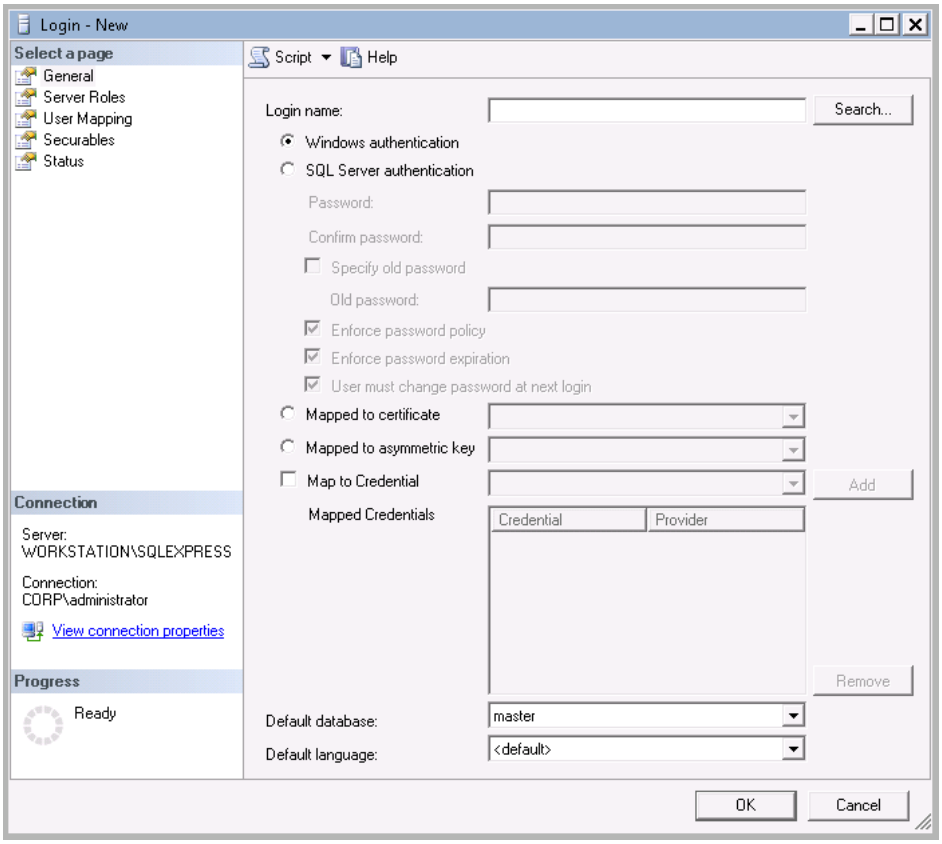
5.3. Define Log On As A Service Policy

On **Managed Object** creation, the **Log on as a service** policy is automatically defined for the Data Processing Account as a local security policy. However, 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, you need to redefine the policy on the domain level through the **Group Policy Management** console.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains** → **<domain_name>**, right-click **Default Domain Policy** and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **User Rights Assignment** and locate the **Log on as aservice** policy.
4. Double-click the **Log on as a service** policy, select **Define these policy settings** and click **Add User or Group**. Specify the account that you want to define this policy for.

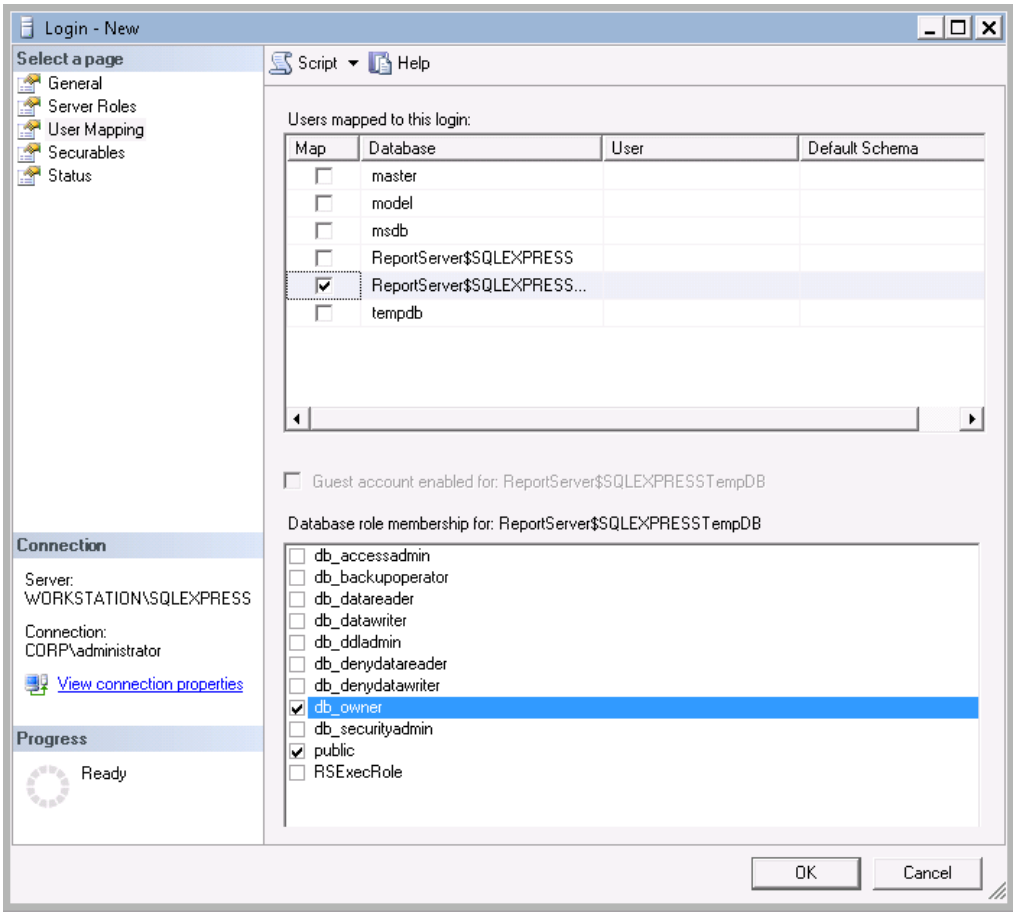
5.4. Assign Database Owner (dbo) Role

1. On the computer where SQL Server with the audit database is installed, navigate to **Start** → **All Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.
2. Connect to the server.
3. In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from the pop-up menu.



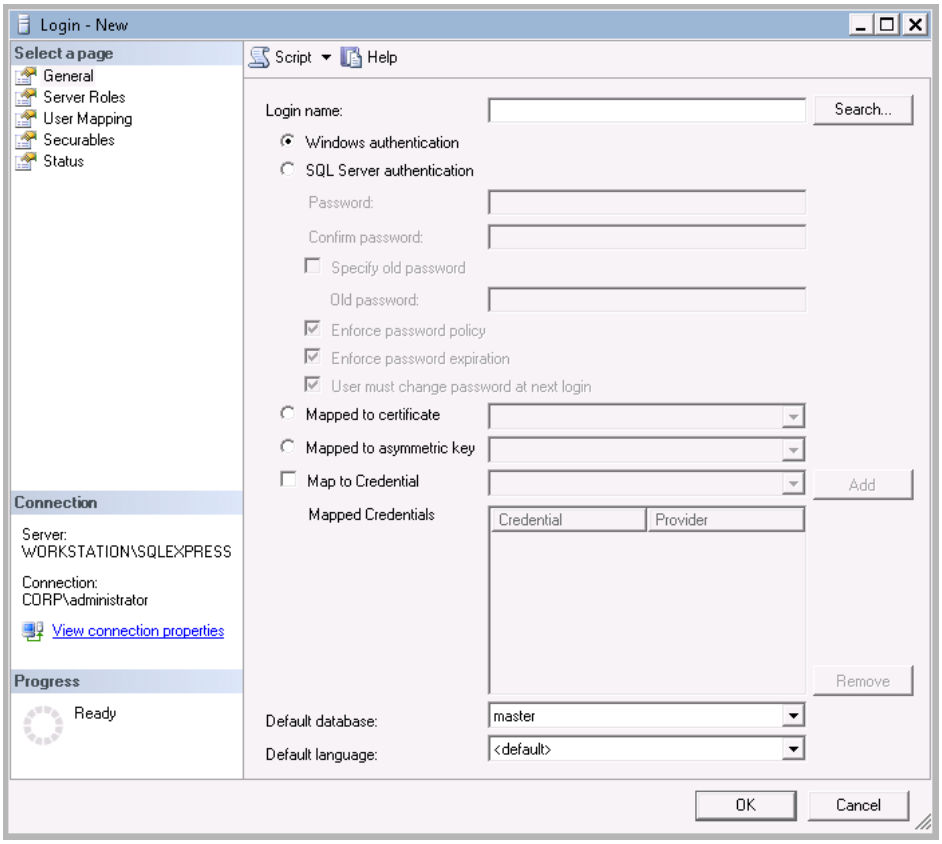
4. Click **Search** next to **Login Name** and specify the user that you want to assign the **dbo** role to.
5. If you are assigning **dbo** role to the Data Processing Account, make sure the **Windows authentication** option is selected. If this is a different account, select **SQL Server authentication**.
6. Select **Server roles** on the left and assign the **sysadmin** role to the new login: all members of this role have the **dbo** role by default. If you do not want to assign the **sysadmin** role to this user, select **public** as server role.
7. Select the **User Mapping** tab. Select the database used by Netwrix Auditor to store audit data in the upper pane and check **db_owner** in the lower pane.

NOTE: If the account that you want to assign the **dbo** role to has already been added to **SQL Server Logins**, expand the **Security** → **Logins** node, right-click the account, select **Properties** from the pop-up menu, and edit its roles.



5.5. Assign System Administrator Role

1. On the computer where SQL Server with the audit database is installed, navigate to **Start** → **All Programs** → **Microsoft SQL Server** → **SQL Server Management Studio**.
2. Connect to the server.
3. In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from the pop-up menu.



4. Click **Search** next to **Login Name** and specify the user that you want to assign the **sysadmin** role to.
5. Specify the **Server roles** tab and assign the **sysadmin** role to the new login.

5.6. Grant Permissions for AD Deleted Objects Container

NOTE: You only need to perform this procedure if the Data Processing Account does not belong to the **domain Administrators** group.

1. Log on to any domain controller in the target domain with a user account that is a member of the **Domain Administrators** group.
2. Navigate to **Start** → **Run** and type *"cmd"*.
3. Input the following command: `dsacls <deleted_object_dn> /takeownership`

   where `deleted_object_dn` is the distinguished name of the deleted directory object.

   For example: `dsacls "CN=Deleted Objects,DC=Corp,DC=local" /takeownership`
4. To grant permission to view objects in the **Deleted Objects** container to a user or a group, type the following command: `dsacls <deleted_object_dn> /G <user_or_group>:<Permissions>`

where `deleted_object_dn` is the distinguished name of the deleted directory object and `user_or_group` is the user or group for whom the permission applies, and `Permissions` is the permission to grant.

For example, `dsacls "CN=Deleted Objects,DC=Corp,DC=local" /G Corp\jsmith:LCRP`

In this example, the user CORP\jsmith has been granted **List Contents** and **Read Property** permissions for the **Deleted Objects** container in the **corp.local** domain. These permissions let this user view the contents of the **Deleted Objects** container, but do not let this user make any changes to the objects in this container. These permissions are equivalent to the default permissions that are granted to the **domain Administrators** group.

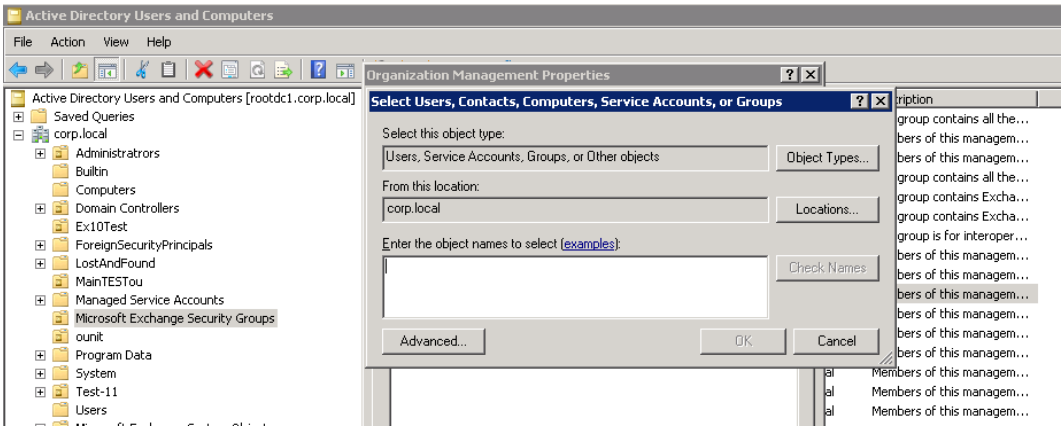
5.7. Assign Permissions To Registry Key

NOTE: You only need to perform this procedure if the Data Processing Account does not belong to the **domain Administrators** group. This procedure must be performed on each domain controller in the audited domain. If your domain contains multiple domain controllers, you may prefer a different method, for example assigning permissions through Group Policy.

1. On your target server, open **Registry Editor:** navigate to **Start** → **Run** and type *"regedit"*.
2. In the left pane, navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security*. Right-click the **Security** node and select **Permissions** from the pop-up menu.
3. Click **Add** and enter the name of the user that you want to grant permissions to.
4. Check **Allow** next to the **Read** permission.

5.8. Add Account to Organization Management Group

1. Navigate to **Start** → **Active Directory Users and Computers** on any domain controller in the root domain of the forest where Microsoft Exchange Server 2010 or 2013 is installed,.
2. In the left pane, navigate to **<domain_name>** → **Microsoft Exchange Security Groups**.
3. On the right, locate the **Organization Management** group and double-click it.
4. In the **Organization Management Properties** dialog that opens, select the **Members** tab and click **Add**.



NOTE: If for some reason you do not want this account to belong to the **Organization Management** group, you can add it to the **Records Management** group in the same way. The **Records Management** group is less powerful, and accounts belonging to it have fewer rights and permissions.

5.9. Assign Audit Logs Role To Account

NOTE: You only need to perform this procedure if you do not want to add the Data Processing Account to the **Organization Management** or the **Records Management** group.

1. On the computer where Microsoft Exchange Server 2010 or 2013 is installed, open the **Exchange Management Shell** under an account that belongs to the **Organization Management** group.
2. Use the following syntax to assign the **Audit Log** role to a user:

   ```
   New-ManagementRoleAssignment -Name <assignment name> -User <UserName> -Role <role name>
   ```

   For example:

   ```
   New-ManagementRoleAssignment -Name "AuditLogsNetwrixRole" -User Corp\jsmith -Role "Audit Logs"
   ```

   In this example, the user CORP\jsmith has been assigned the **Audit Logs** role.

5.10. Assign Content Manager Role To Account

For proper performance of the Reports functionality, the account used to view reports, as well as the account used to run the product scheduled task, must be assigned the Content Manager role for the SSRS Home folder.

1. Start **Report Manager**, open the **Properties** tab of the Home folder and click **New Role Assignment** (the path can slightly vary depending on your SQL Server version).
2. Specify the necessary group or user account in the following format: *domain\user*. The account must

belong to the same domain, or to a trusted domain.

3. Select **Content Manager**.

5.11. Assign SharePoint_Shell_Access Role

The account that runs Netwrix Auditor Agent for SharePoint installation must be granted the **SharePoint_Shell_Access** role on SharePoint SQL Server configuration database. If you select to deploy the agent automatically on the **Create New Managed Object** wizard completion, the installation will be performed under the Data Processing Account.

1. In your SharePoint server click **Start** → **Miscosoft SharePoint Products <version> SharePoint Management Shell**.
2. Execute the following command:

```
Add-SPShellAdmin –UserName <domain\user>
```

6. Upgrade From Previous Versions

You can upgrade your current Netwrix Auditor version to Netwrix Auditor6.0. All your current settings will be preserved and no reconfiguration is required.

NOTE: The upgrade is supported starting from Netwrix Auditor 5.0.x.

To upgrade to Netwrix Auditor 6.0

1. Download Netwrix Auditor 6.0.
2. Open the Netwrix Auditor console. For each of the enabled features under all of your Managed Objects, make sure that the data collection status is not **Running** and disable each feature. If the data collection is in progress, wait until the task completes and then disable the feature.
3. Close all Netwrix Auditor windows.
4. Run the installation package.
5. Click **Install**.
6. Follow the instructions of the setup wizard.

   NOTE: When upgrading from Netwrix Auditor 5.0.80 and below, do not change the program installation path on the **Installation Folder** step of the wizard, otherwise your current configuration may be lost.
7. Netwrix Auditor shortcuts will be added to the **Start** menu and the Netwrix Auditor console will open.

NOTE: When upgrading from Netwrix Auditor 5.0.80 and below to Netwrix Auditor 6.0, the list of installed programs may contain multiple entries for the Inactive User Tracking, Password Expiration Alerting and VMware Auditing features. This does not affect the product operability. Uninstall the older version of the program.

7. Uninstall Netwrix Auditor

7.1. Uninstall Netwrix Auditor

NOTE: If you enabled agents for data collection, make sure to stop them before uninstalling the product. Some agents must be removed manually. See Uninstall Agents for more information.

To uninstall Netwrix Auditor

1. On the computer where Netwrix Auditor is installed, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select the Netwrix Auditor features one by one and click **Uninstall**.

7.2. Uninstall Agents

Some agents are stopped but not removed during Netwrix Auditor uninstallation. You need to delete them manually prior to Netwrix Auditor uninstallation.

Perform the following procedures to uninstall the Netwrix Auditor agents:

- To delete Netwrix Auditor agent for Active Directory Auditing
- To delete Netwrix Auditor agents for Windows Server Auditing
- To delete Netwrix Auditor agents for User Activity Video Recording
- To delete Netwrix Auditor agents for Mailbox Access Auditing
- To delete Netwrix Auditor agents for SharePoint Auditing

To delete Netwrix Auditor agents for Active Directory Auditing

1. On the computer where Netwrix Auditor is installed, navigate to **Start** → **Run** and type *"cmd"*.
2. Execute the following command:

   ```
   %Netwrix_ Auditor_ installation_ folder%\AD Change Reporter Full Version\adcr.exe /removeagents domain=<domain name>
   ```

   where `<domain name>` is the name of the monitored domain in the FQDN format.

   Example:

   ```
   C:\Program Files\Netwrix\AD Change Reporter Full Version\adcr.exe /removeagents domain=domain.local
   ```

3. To delete agents from a specific domain controller, execute the following command:

```
%Netwrix_ Auditor_ installation_ folder%\AD Change Reporter Full
Version\adcr.exe /removeagents dc=<domain controller name
```

To delete Netwrix Auditor agent for Windows Server Auditing

NOTE: Perform this procedure only if you used agents for data collection. Perform this procedure on the computer running Netwrix Auditor before uninstalling the product.

1. On the target servers, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select **Netwrix Windows Server Change Reporter Agent Enterprise Edition** and click **Uninstall**.

To delete Netwrix Auditor agents for User Activity Video Recording

- Remove agents via the Netwrix Auditor console:
    1. In the Netwrix Auditor console, navigate to **Managed Objects** → **<your_managed_object>** in the left pane.
    2. In the right pane select the **Items** tab.
    3. Select a computer in the list and click **Remove**. The agent will be deleted from the selected computer. Perform this action with other computers.
    4. In the left pane navigate to **Managed Objects** → **<your_managed_object>** → **User Session Activity** → **Monitored Computers.** Make sure that the computers you have removed from auditing are no longer present in the list.
    5. In case some computers are still present in the list, select them one by one and click **Retry Uninstallation**. If this does not help, remove the agents manually from the target computers through **Programs and Features**.
- Remove agents manually on each audited computer:
    1. Navigate to **Start** → **Control Panel** → **Programs and Features**.
    2. Select **Netwrix User Activity Video Reporter Agent** and click **Uninstall**.

To delete Netwrix Auditor agents for Mailbox Access Auditing

1. On every computer where a monitored Exchange Server is installed, navigate to **Start** → **Run** and type *"cmd"*.
2. Execute the following command:

    ```
    sc delete "Netwrix Non-owner Mailbox Access Agent"
    ```

3. Remove the following folder: *%Netwrix_Auditor_installtion_folder%\Netwrix Non-owner Mailbox Access Agent*.

To delete Netwrix Auditor agents for SharePoint Auditing

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

1. In the audited SharePoint farm, navigate to the computer where Central Administration is installed and where the agent resides.
2. Navigate to **Start** → **Control Panel** → **Programs and Features**.
3. Select **Netwrix Auditor Agent for SharePoint** and click **Uninstall**.

NOTE: Once you click **Uninstall** you cannot cancel the agent uninstallation. The agent will be uninstalled even if you click **Cancel**.

8. Appendix

This section contains instructions on how to install the third-party components that are not included in the Netwrix Auditor installation package, but are required for the product to function properly.

Refer to the following sections for step-by-step instructions on how to:

- Install Group Policy Management Console
- Install ADSI Edit
- Install Microsoft SQL Server

8.1. Install Group Policy Management Console

Group Policy Management Console is an administrative tool for managing Group Policy across the enterprise.

To use the Group Policy Auditing feature of Netwrix Auditor, Group Policy Management Console must be installed on the computer where the product is deployed.

To install GPMC on Windows 7

1. Download and install **Remote Server Administration 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** → **Feature Administration Tools** and select **Group Policy Management Tools**.
4. Click **Install**.

To install GPMC 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** and select **Group Policy Management**.
3. Click **Install** to enable it.

To install GPMC 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, select **Group Policy Management**.
3. Click **Next** to proceed to confirmation page.
4. Click **Install** to enable it.

To install GPMC 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** → **Feature Administration Tools** and select **Group Policy Management Tools**.

8.2. 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**.

8.3. 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

8.3.1. 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.

8.3.2. 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

V

W