

NETWRIX ACTIVE DIRECTORY CHANGE REPORTER

INSTALLATION AND CONFIGURATION GUIDE

Product Version: 7.1 September/2012

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 discussed. NetWrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice.

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.

© 2012 NetWrix Corporation.

All rights reserved.

Table of Contents

1.	INTRODUCTION
	1.1. Overview
	1.2. How This Guide is Organized 4
	1.3. Free Pre-Sales Support 5
2.	INSTALLATION PREREQUISITES
	2.1. Deployment Options 6
	2.2. Hardware Requirements
	2.3. Software Requirements
	2.4. Supported Environments
	2.5. Supported Microsoft SQL Server Versions
3.	INSTALLING NETWRIX ACTIVE DIRECTORY CHANGE REPORTER PACK
4.	UPGRADING FROM PREVIOUS VERSIONS
5.	UNINSTALLING NETWRIX ACTIVE DIRECTORY CHANGE REPORTER PACK
6.	CONFIGURING TARGET ENVIRONMENT
	6.1. Configuring Target Environment Automatically12
	6.2. Configuring Target Environment Manually16
	6.2.1. Configuring Rights and Permissions
	6.2.2. Configuring Object-Level Auditing
	6.2.3. Adjusting Configuration and Schema Containers Addit Settings
	6.2.5. Configuring Security Event Log Size and Retention Settings
	6.2.6. Configuring Exchange Server AAL Settings
	6.2.7. Adjusting AD Tombstone Lifetime
A	Appendix: Supporting Data
	A.1 Related Documentation

1. INTRODUCTION

1.1. Overview

This guide provides detailed instructions on how to install and set up NetWrix Active Directory Change Reporter. It lists all product requirements and guides you through the installation process.

NetWrix Active Directory Change Reporter can be purchased separately, but it is installed as part of a larger change reporter pack which automates auditing of the entire Active Directory infrastructure.

The NetWrix Active Directory Change Reporter installation package installs the following modules on your computer:

- NetWrix Active Directory Change Reporter
- NetWrix Group Policy Change Reporter
- NetWrix Exchange Change Reporter

This guide contains system requirements for all modules that form the pack, as well as the information on the supported SQL Server versions.

For information on how to configure and use these products, refer to <u>NetWrix Active</u> <u>Directory Change Reporter Administrator's Guide</u>, <u>NetWrix Group Policy Change</u> <u>Reporter Administrator's Guide</u> and <u>NetWrix Exchange Change Reporter</u> <u>Administrator's Guide</u> respectively.

1.2. How This Guide is Organized

This section explains how this guide is organized and provides a brief overview of each chapter.

- Chapter <u>1 Introduction</u> is the current chapter. It explains the purpose of this document, defines its audience and explains its structure.
- Chapter <u>2 Installation Prerequisites</u> lists all product hardware and software requirements, the supported environments and Microsoft SQL Server versions.
- Chapter <u>3 Installing NetWrix Active Directory Change Reporter Pack</u> contains instructions on how to install NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter, and NetWrix Exchange Change Reporter.
- Chapter <u>4 Upgrading from Previous Versions</u> explains how to upgrade the product to the latest released version.
- Chapter <u>5 Uninstalling NetWrix Active Directory Change Reporter Pack</u> provides detailed instructions on how to uninstall the product and remove all of its components.
- Chapter <u>6 Configuring Target Environment</u> explains how to configure your target Active Directory environment for change auditing.
- <u>A Appendix: Supporting Data</u> contains a list of all documentation published to support NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter.

1.3. Free Pre-Sales Support

You are eligible for free technical support during the evaluation period of all NetWrix products. If you encounter any problems, or would like assistance with the installation, configuration or implementation of NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter or NetWrix Exchange Change Reporter, <u>contact NetWrix Technical Support</u>.

2. INSTALLATION PREREQUISITES

This chapter lists all hardware and software requirements for the installation of NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter, and recommendations on how to deploy these products.

2.1. Deployment Options

The NetWrix Active Directory Change Reporter pack can be installed on any computer that belongs to the monitored domain. If you want to monitor several domains, you must establish a trust relationship between these domains and the domain where the product is installed.

The account under which data is collected from trusted domains must have the **Manage auditing and security log** right enabled. For details on how to configure an account for data collection, refer to Section <u>6.2.1 Configuring Rights and</u> <u>Permissions</u>.

2.2. Hardware Requirements

Before installing the NetWrix Active Directory Change Reporter pack, 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, 2GHz
Memory	512MB RAM	4GB RAM
Disk space	 50MB physical disk space for product installation. Additional space is 	Two physical drives with a total of 50GB free space
	 Additional space is required for the Audit Archive and depends on the number of AD objects and changes per day. 	

Table 1: Active Directory Change Reporter Pack Hardware Requirements

2.3. Software Requirements

This section lists the minimum software requirements for the NetWrix Active Directory Change Reporter pack. Make sure that this software has been installed before proceeding with the installation.

Component	Requirement		
Operating System	 Windows XP SP2 (both 32-bit and 64-bit systems) and above 		
Additional software	• .NET Framework <u>2.0</u> , <u>3.0</u> or <u>3.5</u>		
	Windows Installer 3.1 or later		
	Microsoft Management Console 3.0 or later		
	 Group Policy Management Console* 		
	 Windows PowerShell 2.0** 		
	• <u>ASP.Net 2.0</u> **		
	 IIS 5.1 or later (IIS 7.0 or later requires IIS 6 Management Compatibility - all components)*** 		

 Table 2: Active Directory Change Reporter Pack Software Requirements

• Only required for the NetWrix Group Policy Change Reporter module.

** Only required for the NetWrix Exchange Change Reporter module if your monitored domain has an Exchange organization running Microsoft Exchange Server 2010.

*** Only required if you are going to use SQL Server 2005 to store audit data.

2.4. Supported Environments

This section provides a list of AD environments and Microsoft Exchange Server versions supported by NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter.

Component	Version
Active Directory environment	Windows 2000
	 Windows Server 2003 (any forest mode: mixed/native/2k3)
	Windows Server 2008/2008 R2
Microsoft Exchange Server	Microsoft Exchange Server 2003
	Microsoft Exchange Server 2007
	Microsoft Exchange Server 2010

Table 3: Active Directory Change Reporter Pack Supported Environments

2.5. Supported Microsoft SQL Server Versions

Microsoft SQL Server provides the Reporting Services that enable creating, viewing and managing reports based on data stored in a local SQL Server database. NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter use these Reporting Services to generate reports on changes to your Active Directory environment and reports on its configuration snapshots.

To use the Reports functionality, Microsoft SQL Server must be installed on a computer that can be accessed by a NetWrix change reporting product.

The following Microsoft SQL Server versions are supported:

Version	Edition		
SQL Server 2005	 Express Edition with Advanced Services (SP3 or above Standard or Enterprise 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 		

 Table 4: Supported Microsoft SQL Server Versions

SQL Server is not included in the product installation package and must be installed manually or automatically through the Reports Configuration wizard.

For your convenience, we have provided instructions on the manual installation of SQL Server with configuration specific for the Reporting Services to function properly. Refer to the following NetWrix Technical Article for detailed instructions: <u>Installing</u> <u>Microsoft SQL Server and Configuring the Reporting Services</u>.

For full installation and configuration details, refer to the documentation provided by Microsoft.

3. INSTALLING NETWRIX ACTIVE DIRECTORY CHANGE REPORTER PACK

To install NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter, and NetWrix Exchange Change Reporter, perform the following procedure:

Procedure 1. To install the NetWrix Active Directory Change Reporter pack

- 1. <u>Download</u> the NetWrix Active Directory Change Reporter pack.
- 2. Run the setup package called adcrfull_setup.msi.
- 3. Follow the instructions of the installation wizard.
- 4. When prompted, accept the license agreement and specify the installation folder.
- 5. On the last step, click **Finish** to complete the installation.

Shortcuts of all products forming the NetWrix Active Directory Change Reporter pack will be added to your **Start** menu, as well as shortcuts to the following tools:

- Active Directory Object Restore: this wizard provides granular restore capabilities (object- and attribute-level) allowing you to roll back your Active Directory changes using snapshots made by the product, or partially restore Active Directory objects from AD tombstones. For detailed instructions on how to use NetWrix Active Directory Object Restore, refer to Chapter 9 Active Directory Object Restore of <u>NetWrix Active Directory Change Reporter Administrator's Guide</u>.
- Active Directory Audit Configuration: this wizard helps automatically verify and adjust your object-level audit settings, audit policies, rights and permissions, the Security log size and retention settings, and Exchange Server Administrator Audit Logging (required for MS Exchange 2010) in your monitored Active Directory environment. Incorrect audit settings may result in errors in change reports and partial data loss. For more information on the Active Directory Audit Configuration wizard, refer to Section <u>6.1 Configuring Target Environment Automatically</u> of this guide)
- **DB Importer**: this tool is intended for importing data from the Audit Archive to a SQL database. You can use it if you did not enable the Reports functionality on Managed Object creation and decided to save audit data locally, or for data recovery in case your SQL database is corrupted. For detailed instructions on how to use the DB Importer tool, refer to Section 6.2.3. Importing Audit Data to SQL database of <u>NetWrix Active Directory</u> <u>Change Reporter Administrator's Guide</u>.
- **Report Viewer:** this tool allows generating a Change Summary for a selected Managed Object for a specified period of time. For detailed instructions on how to use this tool, refer to Section 5.2.3 Viewing Change Summary for a Specified Date Range of <u>NetWrix Active Directory Change Reporter Administrator's Guide</u>.

4. UPGRADING FROM PREVIOUS VERSIONS

To upgrade NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter, and NetWrix Exchange Change Reporter to the latest released version, perform the following procedure:

Procedure 2. To upgrade the NetWrix Active Directory Change Reporter Pack

- 1. <u>Download</u> the NetWrix Active Directory Change Reporter pack.
- 2. On the computer where the product is installed, close all program windows (NetWrix Enterprise Management Console, wizards, etc.).
- 3. Open the Task Scheduler and disable all Active Directory Change Reporter tasks. Wait until all product processes finish.
- 4. Create a backup of the following folder: %ProgramData%\NetWrix\AD Change Reporter\Rules. This folder contains the NetWrix Active Directory Change Reporter Real-Time Alerts that will be overwritten during the upgrade process.
- 5. Run the setup package called adcrfull_setup.msi.
- 6. When the installation is complete, enable the NetWrix Active Directory Change Reporter tasks in the Task Scheduler.
- 7. Open NetWrix Enterprise Management Console, expand your Managed Object → Active Directory Change Reporter → Real-Time Alerts node and re-enable the alerts that were active before the upgrade process. If you made changes to alert definitions, you can restore them from the backup folder.

All other current product settings will be preserved during the upgrade and no reconfiguration is required.

5. UNINSTALLING NETWRIX ACTIVE DIRECTORY CHANGE REPORTER PACK

To uninstall NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter, and NetWrix Exchange Change Reporter from your computer, perform the following procedures in the order they are provided:

- Delete agents
- <u>Uninstall the product</u>

Procedure 3. To delete agents

- **Note:** It is only necessary to perform this procedure if you used agents for data collection (i.e. the **Network Traffic Compression** option was enabled). Agents are stopped, but not deleted during the uninstallation process, so they have to be removed manually. Perform this procedure on the computer running NetWrix Active Directory Change Reporter before uninstalling the product.
- 1. Navigate to Start \rightarrow Run and type cmd.
- 2. In the command line prompt, execute the following command:

<ADCR_installation_folder>\adcr.exe /removeagents domain=<domain
name>

where $\mbox{-}domain$ name> is the name of the monitored domain in the FQDN format.

E.g.: 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:

```
<ADCR_installation_folder>\adcr.exe /removeagents dc=<domain
controller name>
```

Procedure 4. To uninstall NetWrix the Active Directory Change Reporter pack

- 1. Navigate to Start \rightarrow Control Panel \rightarrow Programs and Features (Add or Remove Programs in Windows 2003).
- 2. Locate NetWrix Active Directory Change Reporter and start the uninstallation wizard. The program will be deleted automatically.

6. CONFIGURING TARGET ENVIRONMENT

Successful change monitoring requires a certain configuration of the audit settings in your monitored Active Directory domain. Otherwise, your change reports may contain errors and incomplete audit data. For example, you can receive a report containing the "System" value instead of an account name in the "Who changed" column.

It is also necessary to assign certain rights and permissions to the Data Processing Account, under which the product scheduled task is run, to be able to collect audit data.

You may also need to adjust your Security event log size to prevent audit data loss if log overwrites occur.

To use the Active Directory Object Restore tool, you need to adjust your AD tombstone lifetime property, so that it agrees with the retention period of the Audit Archive.

You can configure your target environment for change auditing in one of the following ways:

- <u>Automatically</u>
- <u>Manually</u>

6.1. Configuring Target Environment Automatically

You can configure the monitored Active Directory domain automatically, through the Active Directory Audit Configuration wizard.

Note: The AD tombstone lifetime property is not adjusted automatically through the Active Directory Audit Configuration wizard. For instructions on how to configure it manually, refer to Section <u>6.2.7 Adjusting AD</u> <u>Tombstone Lifetime</u> of this guide.

Procedure 5. To configure target environment automatically

 Launch the Active Directory Audit Configuration wizard (Start → All Programs → NetWrix → Active Directory Change Reporter → Active Directory Audit Configuration Wizard).

Note: For the wizard to work properly, you must run it under a Domain admin or an Enterprise admin account.

2. On the first step of the wizard, specify the name of the domain where you want to configure audit settings:



- **Note:** A forest root domain contains audit settings for the Active Directory Configuration and Schema partitions. If you want to monitor changes to Active Directory schema and configuration, and the specified domain is a non-root domain, enable the Also configure forest root domain option. Monitoring of the Configuration partition is enabled by default. For instructions on how to enable monitoring of changes to the Schema partition in NetWrix Active Directory Change Reporter, refer to Section 10.1. Enabling Monitoring of AD Partitions of <u>NetWrix Active Directory</u> <u>Change Reporter Administrator's Guide</u>.
- 3. Click **Next**. In the dialog that appears, select the effective policy that is currently applied to the domain controllers and that is subject to change and click **OK**:
 - Figure 2: Audit Configuration Wizard: Select the Effective Policy

🐔 Active Directory Audit Configuration	×
Select an effective policy, to be applied to the domain controllers of domain "corp.local", from the list below:	
Default Domain Controllers Policy	•
OK Car	ncel

4. On the next step, specify the account that will be used by the product to collect data from the monitored domain.



🐁 Active Directory Audit Configuration .



Click the **Detect** button. A report will be displayed showing your current audit 5. policy settings in the monitored domain as in the example below:



Figure 4: Audit Policy Settings Report

- 6. Click the Adjust button. Your audit policy settings and the Data Processing Account permissions will be adjusted automatically.
- 7. On the next step, repeat these operations for the object-level audit settings. Object-level auditing must be configured so that the "Who" and "When" information appears in audit reports:

Figure 5: Audit Configuration Wizard: Adjust the Object-Level Audit Settings

🐁 Active Directory Audit Configuration -



- 8. On the next step, repeat these operations for your Security event log retention settings. On clicking the **Adjust** button, the size of your Security event log will be set to 300 MB, and the event log auto backup will be enabled if needed:
- Figure 6: Audit Configuration Wizard: Adjust the Event Log Retention Settings

🐁 Active Directory Audit Con	Active Directory Audit Configuration				
	Event Log Retention Settings				
	Step 1: Detect current event log capacity and retention settings. A detailed report will be displayed without changing anything. If you do not have admin rights you can ask the administrator to make changes as per the documentation and click 'Next' to skip step 2 below.				
	Detect				
	modifications to event log retention settings.				
2	If you have already configured these settings, you can skip this step by clicking Next.				
	< Back Next > Cancel				

- 9. On the next step, repeat these operations for the Exchange Server Administrator Audit Logging Settings:
 - **Note:** Configuration of these settings is only required if you are going to use the NetWrix Exchange Change Reporter module, and your monitored AD domain has an Exchange organization running Microsoft Exchange Server 2010.

Figure 7: Audit Configuration Wizard: Adjust the Exchange Server AAL Settings

🐁 Active Directory Audit Configuration



10. On the last step, review your settings and exit the wizard.

6.2. Configuring Target Environment Manually

If you prefer to configure audit settings, rights and permissions, the Security event log size and retention policies, and the AD tombstone lifetime manually, refer to the sections below for detailed instructions:

- **Configuring Rights and Permissions**
- **Configuring Object-Level Auditing**
- Adjusting Configuration and Schema Containers Audit Settings
- **Configuring Domain Controller Audit Policy Settings**
- Configuring Security Event Log Size and Retention Settings
- **Configuring Exchange Server AAL Settings** •
- Adjusting AD Tombstone Lifetime

6.2.1. Configuring Rights and Permissions

To audit object security changes, the Data Processing Account used to collect data from the monitored environment must be a domain admin account or an account with the Manage auditing and security log right enabled.

If you are going to use the NetWrix Exchange Change Reporter module, and your monitored AD domain has an Exchange organization running Microsoft Exchange Server 2010, the Data Processing Account must also belong to the Organization Management or the Records Management group.

The account that will be used to access the SQL database with audit data must belong to the target **Database owner** (dbo) role. You can assign this role to the Default Data Processing Account or any other account of your choice.

Perform the following procedures to configure the Data Processing Account:

- To assign the Manage auditing and security log right
- <u>To assign the Database owner (dbo) role</u>
- To add an account to the Organization Management group

Procedure 6. To assign the Manage auditing and security log right

- 1. Navigate to Start \rightarrow Administrative Tools \rightarrow Group Policy Management.
- 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) node and select Edit from the popup menu.
- 3. In the Group Policy Management Editor, in the left pane, navigate to Computer Configuration → Policies → Windows Settings → Security Settings and select Local Policies.
- 4. On the right, double-click the **User Rights Assignment** policy.
- 5. Locate the Manage auditing and security log right and double-click it. The Manage auditing and security log Properties dialog will be displayed:

Figure 8: Manage Auditing and Security Log Properties Dialog

Manage auditing and security	log Properties	1	? ×
Security Policy Setting Explain			
Manage auditing and	security log		
Define these policy settings:			
Administrators			
Add User or Group	Remove		
	OK	Cancel	Apply

6. Click the Add User or Group button. In the dialog that appears, type in the name of the user that you want to grant this right to and click OK.

Procedure 7. To assign the Database owner (dbo) role

- 1. On the computer where SQL Server is installed, navigate to Start \rightarrow All Programs \rightarrow Microsoft SQL Server \rightarrow SQL Server Management Studio.
- 2. Select the server and click Connect.
- 3. In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from the popup menu. The **Login New** dialog will be displayed:

Select a page	🕞 Carina 🚽 🖾 Units			
😤 General	Scibi • 🚺 Help			
🚰 Server Roles	Login name:			Search
Tuser Mapping		1		
P Status	windows authentication			
_	SQL Server authentication			_
	Password:	1		
	Confirm password:			
	Specify old password			
	Old password:			-
	Enforce password polic	v		
	Enforce password expir	ation		
	User must change pass	word at next login		
	C Mapped to certificate			7
	C Manned to asummetric key	1		
			· · · · · · · · · · · · · · · · · · ·	1
onnection	Map to Credential	1	~	Add
Course	Mapped Credentials	Credential	Provider]
WORKSTATION\SQLEXPRESS				
Connection:				
CORP\administrator				
View connection properties				
rogress				Remove
Ready	Default database:	master	-	·
1943 P	Default language:	<default></default>		-
	5 3-			

Figure 9: Login - New: General

- 4. Click the **Search** button next to the **Login Name** field and specify the user that you want to assign the dbo role to.
- 5. If you are assigning the **Database owner** role to the Data Processing Account, make sure the **Windows authentication** option is selected. If this is a different account, select the **SQL Server authentication** option.
- 6. In the left pane, select Server Roles:

Figure 10: Login - New: Server Roles

🔒 Login - New		_ 🗆 🗙
Select a page	🕵 Script 🔻 🎼 Help	
General Server Roles User Mapping Securables	Server role is used to grant server-wide security privileges to a user.	
ing in Status	Server roles: bulkadnin dbcreator diskadnin processednin poblic securiyadmin setveradnin sysadmin	
Connection		
Server: WORKSTATION\SQLEXPRESS Connection: CORP\administrator		
Progress		
Ready		
	ОК	Cancel

7. You can 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. Then select **User Mapping** in the left pane.

8. Select the database in the upper pane and check **db_owner** in the lower pane:

📑 Login - New					>
Select a page General Server Roles User Mapping Securables Status	Script Users mapp	Help ed to this login: Database master model msdb ReportServer\$SQLEXPRE	User SS	Default	Schema
	Guest a	tempdb	Gerver\$SQLEXPRESST	empDB)
Connection	Database n	ble membership for: Heports	ierver\$SQLEXPHESS1e	mpDB	
Server: WORKSTATION\SQLEXPRESS Connection: CORP\administrator Image: View connection properties	dD_acc db_bac db_data db_data db_ddata db_ddata db_ddata db_ddata db_ddata db_ddata db_ddata db_ddata db_data db	essammin kupoperator areader awriter admin ydatareader ydatawriter ier			
Progress Ready	☐ db_sec ✓ public ☐ RSExec	urityadmin :Role			
				OK	Cancel

Figure 11: Login - New: User Mapping

- 9. Click **OK** to save the changes.
 - **Note:** If the account that you want to assign the **Database owner** role to has already been added to SQL Server Logins, expand the **Security** \rightarrow **Logins** node, right-click this account, select **Properties** from the popup menu, and edit its roles.

Procedure 8. To add an account to the Organization Management group

- 1. On any domain controller in the root domain of the forest where Microsoft Exchange Server 2010 is installed, navigate to Start → Administrative Tools → Active Directory Users and Computers.
- 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 the Add button to add an account to this group:

Figure 12: Organization Management Properties: Add User

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.

6.2.2. Configuring Object-Level Auditing

Object-level Active Directory auditing must be configured so that the "Who" and "When" information appears in audit reports. To do this, perform the following procedure:

Procedure 9. To configure Active Directory auditing

 Navigate to Start → Programs → Administrative Tools → Active Directory Users and Computers. In the Active Directory Users and Computers dialog, click View in the main menu and ensure that the Advanced Features option is selected.

📔 Active Dire	ctory Users and Computers	
File Action	View Help	
(= -) 🖄	Add/Remove Columns	3 <u>8</u>
Active Direc	Large Icons	Description
E 📑 Soved C	List Detail	Default container for upgr Default container for dom
	Users, Contacts, Groups, and Computers as containers	Default container for secu Default container for orph
	V Advanced Peatores	Default container for man Default location for storag
	Customize	Builtin system settings
•	Users Container NTDS Quotas msDS-QuotaCo Infrastructure infrastructureU.	Default container for upgr Quota specifications cont
Enables/disables	advanced features and objects	

Figure 13: Active Directory Users and Computers Dialog

2. Right-click the <domain_name> node and select **Properties**. In the domain Properties dialog, open the **Security** tab and click the **Advanced** button. The **Advanced Security Settings** dialog will open. Select the **Auditing** tab:

Figure 14: Advanced Security Settings: Auditing

L	Advanced Security Settings for corp 🛛 🛛 🗙						
ŀ	Permissions Auditing Owner Effective Permissions						
	To view or edit details for an auditing entry, select the entry and then click Edit.						
	Auditing entrie	s:					
	Туре	Name	Access	Inherited From	Apply To		
	Success	Everyone	Special	<not inherited=""></not>	This object only		
	Success	Administrators (CORP\Ad	All extended rights	<not inherited=""></not>	This object only		
	Success	Domain Users (CORP\Do	All extended rights	<not inherited=""></not>	This object only		
	Success	Everyone		<not inherited=""></not>	Special		
	Success	Everyone		<not inherited=""></not>	Special		
	·						
	Add	Edit	Remove		Restore defaults		
	What are the requirements for auditing object access?						
				ОК	Cancel Apply		

- 3. Press the Add button. In the Select user, Computer, Service account, or Group dialog, type 'Everyone' in the Enter the object name to select entry field and click OK.
- 4. 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:

Name: Everyone Apply onto: This object and all de	escendant objects	Change
Access: Full control List contents Read all properties Write all properties Delete Delete subtree Read permissions Modify permissions Modify owner All validated writes All extended rights Apply these auditing entries to only Managing auditing	Successful	Clear All

Figure 15: Audit Entry Dialog

- 5. Make sure that the Apply these auditing entries to objects and/or containers within this container only check-box is *not* selected. Also, make sure that the Apply onto parameter is set to This object and all descendant objects.
- 6. Click **OK** to save the changes.

6.2.3. Adjusting Configuration and Schema Containers Audit Settings

If you want to track changes to the domain Configuration and/or Schema containers, you must enable object-level auditing for these containers. To do this, perform the following procedure:

Procedure 10. To enable object-level auditing for the Configuration and Schema containers

- **Note:** To perform this procedure, you will need the <u>ADSI Edit</u> utility. In Windows 2003 systems, this utility is a component of Windows Server Support Tools. If it has not been installed, download Windows Server Support Tools from the official website. On Windows 2008 systems and above, this component is installed together with the AD DS role.
- 1. Navigate to Start \rightarrow Programs \rightarrow Administrative Tools \rightarrow ADSI Edit. The ADSI Edit dialog will open.



Figure 16: ADSI Edit dialog

2. Right-click the ADSI Edit node and select the Connect To option. In the Connection Settings dialog, enable the Select a well-known Naming Context option and select Configuration from the drop-down list. Click OK:

Connection Settings
Name: Configuration
Path: LDAP://adminDC1.company.local/Configuration
Connection Point
Select or type a Distinguished Name or Naming Context:
Select a well known Naming Context:
Configuration
Computer
Computer © Select or type a domain or server: (Server Domain [:port])
Computer C Select or type a domain or server: (Server Domain [:port])
Computer C Select or type a domain or server: (Server Domain [:port]) C Default (Domain or server that you logged in to)
Computer C Select or type a domain or server: (Server Domain [:port]) C Default (Domain or server that you logged in to) C type ST is a server that you logged in to)
Computer C Select or type a domain or server: (Server Domain [:port]) Default (Domain or server that you logged in to) Use SSL-based Encryption
Computer C Select or type a domain or server: (Server Domain [:port]) C Default (Domain or server that you logged in to) Use SSL-based Encryption Advanced OK Cancel

Figure 17: Connection Settings Dialog

- 3. Expand the Configuration <Your_Root_Domain_Name > node. Right-click the CN=Configuration, DC=... node and select Properties.
- In the CN=Configuration, DC=company, DC=local Properties dialog select the Security tab and press the Advanced button. In the Advanced Security Settings for Configuration dialog open the Auditing tab and press the Add button.
- 5. In the Select User, Computer, Service Account, or Group dialog type 'Everyone' in the Enter the object name to select entry field and click OK. The Auditing Entry for Configuration dialog will open.
- 6. Set the **Successful** parameter for all access entries except the following: Full Control, List Contents, Read All Properties and Read Permissions:

📙 Auditing Entry for Configuration		
Object Properties		
. 1		
Name: Everyone		⊆hange
Apply onto: This object and all desce	endant objects	•
, Access:	Successful	Failed
Full control List contents Read all properties Write all properties Delete Delete subtree Read permissions Modify permissions Modify owner All validated writes All extended rights		
Apply these auditing entries to ob ad/or containers within this cont only <u>Managing auditing</u>	ijects ainer	Clear All
	OK	Cancel

Figure 18: Auditing Entry for Configuration Dialog

7. Make sure that the **Apply these auditing entries to objects and/or containers within his container only** check-box is *not* selected. Also, make sure that the **Apply onto parameter** is set to **This object and all descendant objects**.

- 8. Click **OK** to save the changes.
- 9. Repeat steps 2-8 for the Schema container if necessary.

6.2.4. Configuring Domain Controller Audit Policy Settings

For the product to collect audit data correctly, you must enable the **Audit directory service access** and the **Audit account management** policies. To do this, perform the following procedure:

Procedure 11. To configure audit policy settings

 Navigate to Start → Programs → Administrative Tools → Group Policy Management. The Group Policy Management dialog will open:

📓 Group Policy Management	
File Action View Window Help	_ B ×
Image: Group Policy Management Image: Construction of the state	Croup Policy Management Contents Name Forest: company.local

Figure 19: Group Policy Management Console

- 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 popup menu.
- In the Group Policy Management Editor dialog, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy.
- 4. Ensure that the Audit account management and Audit directory service access options are set to Success (or Success and Failure):

🗐 Group Policy Management Editor		
	Policy Audit account logon events Audit account management Audit directory service access Audit logon events Audit object access Audit policy change Audit policy change Audit porcess tracking Audit system events	Policy Setting Success Success Not Defined Success No auditing No auditing Success
Event Log		

Figure 20: Group Policy Management Editor Dialog

6.2.5. Configuring 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 MBs (according to the following Microsoft Knowledge Base article: <u>Event log may not grow to configured size</u>), 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.

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

- Increase the maximum size of the Security event log and set its retention method
- Enable event log Auto archiving
- Configure backup logs retention

Procedure 12. To increase the maximum size of the Security event log and set its retention method

 Navigate to Start → Programs → Administrative Tools → Group Policy Management. The Group Policy Management dialog will open:

🔜 Group Policy Management	
File Action View Window Help File Action View Window Help Group Policy Management Group Policy Management Sites Group Policy Modeling Group Policy Results	Group Policy Management Contents Name Forest: company.local

Figure 21: Group Policy Management Console

- 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 popup menu.
- 3. Navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Event Log:

Elle Action View Help		
 Default Domain Controllers Policy [ADMINDC1 Computer Configuration Policies Software Settings Windows Settings Scripts (Startup/Shutdown) Security Settings Account Policies Local Policies Event Log Restricted Groups System Services System Services 	Policy Maximum application log size Maximum system log size Maximum system log size Prevent local guests group from accessing application log Prevent local guests group from accessing security log Prevent local guests group from accessing system log Retain application log Retain security log Retain security log Retention method for application log Retention method for system log Retention method for system log 	Policy Setting Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Manually Not Defined
	<u>.</u>	

Figure 22: Group Policy Management Editor Dialog

4. Double-click Maximum security log size. In the Maximum security log size Properties dialog, select the Define this policy setting option and set Maximum security log size to 299968 kilobytes.

Figure 23: Maximum security log size Properties Dialog

Maximum security log size Properties	? ×
Security Policy Setting Explain	
Maximum security log size	
Define this policy setting	
299968 💼 kilobytes	
Modifying this setting may affect compatibility with clients, services, and applications. For more information, see <u>Maximum security log size</u> . (Q823659)	
OK Cancel App	y I

- 5. Click **OK** to save the changes.
- 6. Double-click **Retention method for security log**. In the **Retention method for security log Properties** dialog, select the **Define this policy setting** option and select **Overwrite events as needed**:

Figure 74:	Retention method	for security	log Pro	nerties Dialog
i igui e z i.	Recención mechoa	joi securicy	103110	per cies bialog

Retention m	ethod for security	log Properties	5	? ×
Security Poli	cy Setting Explain			
F	Retention method for	security log		
🔽 Define	this policy setting			
O 0v	erwrite events by day	15		
• 0v	erwrite events as nee	eded		
O Do	not overwrite events	(clear log manua	lly)	
 Overwrite events as needed Do not overwrite events (clear log manually) Modifying this setting may affect compatibility with clients, services, and applications. For more information, see <u>Retention method for security log</u>. (Q823659) 				
		OK	Cancel	Apply

- 7. Click **OK** to save the changes.
- 8. Navigate to Start \rightarrow Run and execute the "cmd" command. Type the "gpupdate" command and press Enter. The group policy will be updated.

Procedure 13. To enable Auto archiving centrally on all Domain Controllers

Note: This procedure can be performed on any domain controller.

- 1. Navigate to Start \rightarrow Programs \rightarrow Administrative Tools \rightarrow 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 popup menu.
- 3. Navigate to Computer Configuration → Policies. Right-click Administrative Templates: Policy definitions and select Add/remove templates. In the Add/Remove Templates dialog, click the Add button.
- 4. In the **Policy Templates** dialog, navigate to the Active Directory Change Reporter installation directory, 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**.
- 5. Click the Close button in the Add/Remove Templates dialog.
 - **Note:** If you are running Widows Server 2003 or below, after step 4, click View in the Main menu, select Filtering and deselect the Only show policy settings that can be fully managed option.
- 6. Navigate to Administrative Templates: Policy definitions \rightarrow Classic Administrative Templates \rightarrow System \rightarrow Event Log.
- 7. Double-click Automatically clear a full security event log and back up the log file. Select the Enabled option and click OK to save the changes.

- 8. Navigate to Start \rightarrow Run and execute the 'cmd' command. Type the 'gpupdate' command and press Enter. The group policy will be updated.
 - **Note:** Depending on the activity in the monitored environment, the Security log auto backup files can fill the free space on your disk drive before the product removes them. To prevent disk drive overfilling, if needed, change the behavior of the backup logs by performing <u>Procedure 14 To configure the retention period for the backup logs</u> below.

Procedure 14. To configure the retention period for the backup logs

- **Note:** Perform this procedure on the computer where NetWrix Active Directory Change Reporter is installed.
- 1. Navigate to Start \rightarrow Run, type the 'regedit' command and click OK.
- 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.
- 4. This value defines the time period (in hours) after which archives will be deleted automatically. By default, it is set to 50 (decimal). Modify this value, if necessary, and click **OK** to save the changes.

Edit DWORD (32-bit) Value	x
Value name:	
CleanAutoBackupLogs	
Value data:	Base
80	O Hexadecimal
	Decimal
	OK Cancel

Figure 25: Edit DWORD Value Dialog

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.

6.2.6. Configuring Exchange Server AAL Settings

If you are going to use the NetWrix Exchange Change Reporter module, and your monitored domain has an Exchange organization running Microsoft Exchange Server 2010 SP1, you must configure the Exchange server Administrator Audit Logging (AAL) settings. To do this, perform the following procedure:

Procedure 15. To configure Exchange Server AAL settings

- 1. On the computer where the target Microsoft Exchange Server 2010 is installed, navigate to Start → Programs → Exchange Management Shell.
- 2. Execute the following command:

```
[PS] C:\Windows\system32>Set-AdminAuditLogConfig -
AdminAuditLogEnabled $true -AdminAuditLogAgeLimit 30 -
AdminAuditLogCmdlets *
```

- 3. On the computer where NetWrix Exchange Change Reporter is installed, browse to the product installation 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
```

- 5. On the computer where the target Exchange Server 2010 is installed, navigate to Start \rightarrow Administrative Tools \rightarrow Internet Information Services (IIS) Manager.
- 6. In the left pane, navigate to <server_name> \rightarrow Sites \rightarrow <site_name> \rightarrow PowerShell and double-click Application Settings in the right pane:

A									
/Po	werShell	Home							
Filter: • 🗑 Go - 🐙 Show All Group by: Area • 📰 •									
ASP.NET									
=		404	٢				i 🕵	1	ab
.NET Authorizati	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	.NET Users	Application Settings	Connection Strings
7		R	&	•					
Machine Key	Pages and Controls	Providers	Session State	SMTP E-mail					
115									
	Ð	ø	<u> </u>	404		2			
Authentication	Compression	Default Document	Directory Browsing	Error Pages	Failed Request Tracing Rules	Handler Mappings	HTTP Redirect	HTTP Respo	Logging
			8	9					
MIME Types	Modules	Output Caching	Request Filtering	SSL Settings					
Manageme	nt								
Configuration Editor									

Figure 26: IIS Manager: PowerShell Home

- 7. In the Application Settings page, double-click the PSLanguageMode parameter and set its value to 'FullLanguage'.
- In the left pane, navigate to <server_name> → Application Pools. Select MSExchangePowerShellAppPool on the right, and click Recycle in the Actions pane:

Application Book					Ac	Actions		
This page lets you view and manage the list of ap	plication po	ols on the	server, Application pools are	e associated with		Add Application Pool Set Application Pool Defaults		
Filter:	ihow All	Group by:	No Grouping	•	▶	Application Pool Tasks Start		
Name 🔺	Status	.NET Fr	ame Managed Pipeli	Identity		Stop		
Classic .NET AppPool	Started	v2.0	Classic	ApplicationPoolIden	2	Recycle		
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIden		Edit Application Real		
MSExchangeAutodiscoverAppPool	Started	v2.0	Integrated	LocalSystem		Edit Application Poor		
MSExchangeECPAppPool	Started	v2.0	Integrated	LocalSystem		Basic Settings		
MSExchangeOWAAppPool	Started	v2.0	Integrated	LocalSystem		Recycling		
MSExchangeOWACalendarAppPool	Started	v2.0	Integrated	LocalSystem		Advanced Settings		
MSExchangePowerShellAppPool	Started	v2.0	Integrated	LocalSystem		Rename		
MSExchangeServicesAppPool	Started	v2.0	Integrated	LocalSystem		-		
MSExchangeSyncAppPool	Started	v2.0	Integrated	LocalSystem	^	Remove		
						View Applications		
					2	Help		
						Online Help		

Figure 27: IIS Manager: Application Pools

Note: Steps 1-4 (AAL configuration) of this procedure can be performed on any of the monitored Exchange servers, as these settings will then be replicated to all Exchange servers in the domain. Steps 5-8 (IIS configuration) must be performed on each of the monitored Exchange servers.

6.2.7. Adjusting AD Tombstone Lifetime

You can restore deleted Active Directory objects and their attributes using the Active Directory Object Restore tool integrated with NetWrix Active Directory Change Reporter. 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 AD objects, you must adjust the AD tombstone lifetime property (set by default to 60 days in Windows 2003 and to 180 days in Windows 2008 and higher) so that it agrees with the Audit Archive retention period (2 years by default).

Procedure 16. To change the tombstone lifetime attribute

- **Note:** To perform this procedure, you will need the <u>ADSI Edit</u> utility. In Windows 2003 systems, this utility is a component of Windows Server Support Tools. If it has not been installed, download Windows Server Support Tools from the official website. On Windows 2008 systems and above, this component is installed together with the AD DS role.
- 1. Navigate to Start \rightarrow Programs \rightarrow Administrative Tools \rightarrow ADSI Edit. The ADSI Edit dialog will open.

Figure 28: ADSI Edit dialog



2. Right-click the **ADSI Edit** node and select the **Connect To** option. In the **Connection Settings** dialog, enable the **Select a well-known Naming Context** option and select **Configuration** from the drop-down list. Click **OK**:

Figure 29: Connection Settings Dialog

Connecl	tion Settings	х
		_
<u>N</u> ame:	Configuration	
		_
<u>P</u> ath:	LDAP://adminDC1.company.local/Configuration	
Conn	ection Point	
09	Select or type a <u>D</u> istinguished Name or Naming Context:	
	•	
	Select a well known N <u>a</u> ming Context:	
	K optiquiration	
Comp	Lonriguration	
Comp	Jcontriguration	
Comp	Select or type a domain or server: (Server Domain [:port])	
Comp C s	Source Server (Server Domain [:port])	
Comp	Select or type a domain or server: (Server Domain [:port])	
	Jcontriguration	
	Select or type a domain or server: (Server Domain [:port])	

- In the left pane, navigate to Configuration <Your_Root_Domain_Name> → CN=Configuration,DC=corp,DC=local → CN=Services → CN=Windows NT → CN=Directory Service node. Right-click it and select Properties from the popup menu.
- 4. In the **CN=Directory Service Properties** dialogue, in the **Attribute Editor** tab, locate the tombstoneLifetime attribute:





- 5. Select this attribute and click the Edit button.
- 6. In the dialogue that opens, set the value of this attribute to 730 (which equals 2 years).

A APPENDIX: SUPPORTING DATA

A.1 Related Documentation

The table below lists all documents available to support NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter:

Document Name	Overview
NetWrix Active Directory Change Reporter Installation and Configuration Guide	The current document
NetWrix Active Directory Change Reporter Administrator's Guide	Provides a detailed explanation of the NetWrix Active Directory Change Reporter features and step-by-step instructions on how to configure and use the product.
NetWrix Group Policy Change Reporter Administrator's Guide	Provides a detailed explanation of the NetWrix Group Policy Change Reporter features and step-by-step instructions on how to configure and use the product.
NetWrix Exchange Change Reporter Administrator's Guide	Provides a detailed explanation of the NetWrix Exchange Change Reporter features and step-by-step instructions on how to configure and use the product.
NetWrix Active Directory Change Reporter Freeware Edition Quick-Start Guide	Provides instructions on how to install, configure and use NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter Freeware Edition.
NetWrix Active Directory Change Reporter Release Notes	Contains a list of the known issues that customers may experience with NetWrix Active Directory Change Reporter 7.1, and suggests workarounds for these issues.

Table 5: Product Documentation