

NETWRIX WINDOWS SERVER CHANGE REPORTER

ADMINISTRATOR'S GUIDE

Product Version: 4.0

June 2013

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.

© 2013 Netwrix Corporation.

All rights reserved.

Table of Contents

1.	INTRO	DUCTION	. 5
	1.1.	Overview	. 5
	1.2.	How This Guide is Organized	. 5
2.	Prod	UCT OVERVIEW	. 6
	2.1.	Key Features and Benefits	. 6
	2.2.	Product Workflow	. 7
	2.3.	Product Editions	. 8
3.	Νετω	RIX MANAGEMENT CONSOLE OVERVIEW	. 9
4.	MANA	GED OBJECT	10
	4.1.	Creating Managed Object	. 10
	4.2.	Modifying Managed Object Settings	. 22
5.	Data		26
	5.1.	Data Collection Workflow	. 26
	5.2.	Change Summary	.27
		5.2.1. Generating Change Summary on Demand	. 27
		5.2.2. Viewing Change Summary for the Specified Time Frame	. 28
	5.3.	Sessions	. 30
6.	Repo	RTS	31
	6.1.	Reports Overview	. 31
	6.2.	Configuring Reports	. 32
		6.2.1. Specifying SQL Server Settings	. 32
		6.2.2. Uploading Report Templates to the Report Server	. 35
		6.2.3. Importing Audit Data to SQL Database	. 35
	6 2	Viewing Deports	0C.
	0.3.	6 3 1 Viewing Reports in Netwrix Management Console	0C.
		6.3.2. Viewing Reports in Web Browser	. 40
	6.4.	Configuring Report Subscriptions	. 42
		6.4.1. Creating a Subscription	. 42
		6.4.2. Modifying a Subscription	. 46
	<u>۲</u> ۲	0.4.3. Forcing On-Demand Report Delivery	40
	0.J.		.4ŏ
	6.6.	Change Management	. 50
			-117

7.	CONFIGURING GLOBAL SETTINGS	53
	7.1. Configuring the Reports Settings	54
	7.2. Configuring the Email Notifications Settings	55
	7.3. Configuring Audit Archive Settings	56
	7.4. Configuring Data Collection Settings	57
	7.5. Configuring License Settings	59
	7.6. Configuring Netwrix Console Audit	60
8.	Additional Configuration	63
	8.1. Configuring Integration with Netwrix User Activity Video Reporter	63
	8.2. Excluding/Including Data Types from/in Reports	66
Α	APPENDIX: MONITORED COMPONENTS AND SETTINGS	67
	A.1 General Computer Settings	67
	A.2 Add/Remove Programs	67
	A.3 Services	68
	A.4 Hardware	68
	A.5 Scheduled Tasks	72
	A.6 Local Users and Groups	72
	A.7 DNS Configuration*	72
	A.8 DNS Resource Records*	74
	A.9 Windows Registry Settings	78
В	APPENDIX: RELATED DOCUMENTATION	84

1. INTRODUCTION

1.1. Overview

This guide contains an overview of the Netwrix Windows Server Change Reporter functionality and features, and detailed step-by-step instructions on how to configure and use the product. For instructions on how to install the product and configure the target computers for audit, refer to <u>Netwrix Windows Server Change Reporter Installation and Configuration Guide</u>.

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>: the current chapter. It explains the purpose of this document and explains its structure.
- Chapter <u>2 Product Overview</u> provides an overview of the Netwrix Windows Server Change Reporter functionality, lists its main features and benefits, and explains the product workflow. It also contains the information on the product editions and a side-by-side comparison of their features.
- Chapter <u>3 Netwrix Management Console Overview</u> provides a description of Netwrix Management Console, which is an integrated interface for most Netwrix products.
- Chapter <u>4 Managed Object</u> explains how to configure a Managed Object. It also explains how to modify Managed Object settings.
- Chapter <u>5 Data Collection</u> explains the Netwrix Windows Server Change Reporter data collection workflow and contains detailed information on the Change Summary options and Sessions.
- Chapter <u>6 Reports</u> provides an overview of the Reports feature, explains how to configure and view reports and contains report examples. It also contains step-by-step instructions on how to configure subscriptions to Reports.
- Chapter <u>7 Configuring Global Settings</u> explains how to configure or modify the settings that are applied to all Managed Objects and all Netwrix modules enabled for these objects.
- Chapter <u>8 Additional Configuration</u> provides a description of the product additional configuration options, such as enabling integration with Netwrix User Activity Video Reporter and excluding data types from data collection and product reports.
- <u>A Appendix: Monitored Components and Settings</u> lists all system components and settings monitored by Netwrix Windows Server Change Reporter.
- <u>B Appendix: Related Documentation</u> contains a list of all documents published to support Netwrix Windows Server Change Reporter.

2. PRODUCT OVERVIEW

Netwrix Windows Server Change Reporter allows automatic tracking of configuration changes made to Windows servers. This solution assists in monitoring of all critical Windows-based systems within the organization, and across multiple sites and Active Directory forests. Basing on Netwrix technologies, this tool produces clear and concise reports for IT managers and security auditors.

Netwrix Windows Server Change Reporter audits changes in such system components as general computer settings, hardware, software, services, scheduled tasks, local users and groups, Windows Registry, DNS configuration, and others. For the full list of monitored components, refer to <u>A Appendix: Monitored Components and Settings</u>.

2.1. Key Features and Benefits

Netwrix Windows Server Change Reporter allows you to do the following:

- Monitor day-to-day administrative activities: the product captures detailed information on all changes made to the monitored environment, including the information on WHO changed WHAT, WHEN and WHERE.
- **Sustain compliance** by using in-depth change information. Audit data can be archived and stored for more than 7 years to be used for reports generation.
- **Centralize audit trail:** audit data on Windows server configuration changes is stored in a central location, and the usage of the <u>AuditAssurance™ and AuditIntelligence™</u> <u>technologies</u> allows collecting data from multiple sources and converting it into a set of single strings forming a report in a human-readable format.
- Quickly implement and configure a monitoring tool for new instances: Windows server environment is subjected to frequent changes complicating the monitoring and auditing tasks. Netwrix Windows Server Change Reporter allows adapting quickly to the constantly changing demands. The simplified installation and configuration allow system administrators to start auditing Windows server configuration in as little as 15 minutes.

Netwrix Windows Server Change Reporter has the following main features:

- The single tool allows monitoring a big variety of system components for critical configuration changes.
- Reports containing the details on the previous and current values of the configuration settings that are subjected to changes.
- Report Subscriptions allow configuring any available reports for automatic delivery by specifying the report filters, recipients, delivery format and schedule.
- The Overview report provides immediate access to important statistics in a chart format. It is linked to specific reports that take you to the next level of detail by means of the drill-through functionality.
- Long-term data storage allows retrieving historical data on configuration changes at any time. The retention period can be adjusted to your needs and compliance regulations.

2.2. Product Workflow

A typical Netwrix Windows Server Change Reporter data collection and reporting workflow is as follows:

- 1. An administrator configures Managed Objects and sets the parameters for automated data collection and reporting.
- 2. Netwrix Windows Server Change Reporter monitors the target servers and collects audit data on configuration changes. Audit data is written to a local file-based storage, referred to as Audit Archive.
- 3. The product emails Change Summaries containing a list of all changes that occurred in the last 24 hours to the specified recipients daily at 3:00 AM by default.
- 4. If the Reports functionality is enabled and configured, data is imported from Audit Archive to a dedicated SQL database. Detailed audit reports with grouping, sorting and filtering capabilities can be viewed via Netwrix Management Console or in a web browser.

2.3. Product Editions

Netwrix Windows Server Change Reporter is available in two editions: Freeware and Enterprise. The Freeware Edition can be used by companies or individuals for an unlimited period of time. The Enterprise Edition can be evaluated free of charge for 20 days.

<u>Table 1:</u> below outlines the differences between the Netwrix Windows Server Change Reporter Editions:

Feature	Freeware Edition	Enterprise Edition
WHAT and WHERE fields for every change	Yes	Yes
WHO and WHEN fields for every change	No	Yes
The before and after values for every change	Yes	Yes
Reports based on SQL Server Reporting Services, with filtering, grouping and sorting	No	Yes
Custom reports	No	Yes Create manually or <u>order from Netwrix</u>
Monitoring of local users and groups changes	No	Yes
Monitoring of Windows Registry changes	No	Yes
Monitoring of changes to DNS Server configuration and resource records	No	Yes
SMTP authentication and SSL	No	Yes
Automatic audit configuration on target computers	No	Yes
Report subscriptions	No	Yes
Long-term archiving of audit data	No Data is only stored for 2 days	Yes Any period of time
Daily Change Summary email reflecting the changes made in the last 24 hours	Yes	Yes
A single installation handles multiple Managed Objects, each with its own individual settings	No	Yes
Integrated interface for all Netwrix products, which provides centralized configuration and settings management	No	Yes
Reports can be viewed directly from Netwrix Enterprise Management Console	No	Yes
Technical Support	<u>Support Forum</u> <u>Knowledge Base</u>	Full range of options: Phone, email, submission of support tickets, Support Forum, Knowledge Base
Licensing	Free of charge	Per server Request a quote

Table 1: Netwrix Windows Server Change Reporter Editions

3. NETWRIX MANAGEMENT CONSOLE OVERVIEW

Netwrix Windows Server Change Reporter Enterprise Edition is integrated into Netwrix Management Console, an MMC snap-in that allows configuring Managed Objects and their settings, and the reporting options.

Netwrix Management Console enables you to do the following:

- <u>Manage the settings of all Netwrix change auditing products via an integrated</u>
 <u>interface</u>
- <u>Create and configure Managed Objects</u>
- Enable and configure SSRS-based Reports
- <u>View Reports</u>
- <u>Configure long-term archiving</u>
- <u>Configure Subscriptions to Reports</u>
- Handle numerous Managed Objects with a single installation
- Configure your Managed Objects settings in a batch

To start Netwrix Management Console, navigate to Start \rightarrow All Programs \rightarrow Netwrix \rightarrow Netwrix Management Console. The console window will be displayed:

📑 NetWrix Enterprise Managemen	t Console	
File Action View Help		
(=		
 WetWrix Enterprise Management Co Managed Objects Settings All Sessions 	systems Management and Complexes	Management Console
	Welcome to NetWrix Enterprise Managem The console is an integrated interface for NetWrix pro server, computer collection, and so on), manage your	Ient Console ducts allowing you to define the scope of your monitored environment (AD domain, OU, file data collection settings, configure and view audit reports.
	Create New Managed Object This wizard helps you create a Managed O audit data you want to collect.	bject. You can enable different modules for your Managed Objects depending on the type of
	Installed Modules Select a module below to create a new M	anaged Object.
	Windows Server Change Reporter	Auditing of who changed what, where and when in Windows servers configuration: registry settings, hardware, software, local groups, WMI, etc. <u>Configure</u>
	Get More The following modules are available for d	ownload:
	Active Directory Change Reporter	Tracking, reporting and real-time alerting on who changed what, when and where in Active Directory objects and settings.
	Group Policy Change Reporter	Tracking and reporting on who changed what, when and where in Group Policy objects and settings.
	Exchange Change Reporter	Learn More Tracking and reporting on who changed what, when and where in Exchange Server configuration, permissions and other settings.
	Inactive Users Tracker	Learn More Automatic detection and deactivation of inactive user and computer accounts in Active Directory.
× • •	Assword Expiration Notifier	Learn More Automatic delivery of notifications to non-interactive users with expiring passwords prompting them to change their passwords.

Figure 1: Netwrix Management Console

4. MANAGED OBJECT

In Netwrix Windows Server Change Reporter, a Managed Object is a Computer Collection that is monitored for changes.

This chapter provides detailed step-by-step instructions on how to:

- Create and configure a Managed Object
- <u>Modify Managed Object settings</u>

4.1. Creating Managed Object

To create and configure a Managed Object, do the following:

Procedure 1. To create and configure a Managed Object

1. In Netwrix Management Console, select the **Managed Objects** node in the left pane. The **Managed Objects** page will be displayed:

🖷 NetWrix Enterprise Management Cons	NetWrix Enterprise Management Console		
File Action View Help			
🗢 🔿 🖄 📷 🚺 🖬			
 WetWrix Enterprise Management Console 	Pythem Management and Complexes Enterprise Management Console		
	Managed Objects — Start by configuring one or several Managed Objects. Managed Objects can be grouped into folders.		
	Create New Managed Object This wizard helps you create a Managed Object. You can enable different modules for your Managed Objects depending on the type of audit data you want to collect.		
	Create New Folder — Create a folder to group your Managed Objects.		

Figure 2: Managed Objects Page

- 2. Click **Create New Managed Object** in the right pane. Alternatively, right-click the **Managed Objects** node and select **New Managed Object** from the popup menu to start the **New Managed Object** wizard.
 - **Note:** For your convenience, you can group Managed Objects into folders. To create a folder, right-click the **Managed Objects** node, select **New Folder**, and specify the folder name. Then create a new Managed Object inside this folder. You cannot move existing Managed Objects into folders once they have been created.
- 3. On the Select Managed Object Type step, select Computer Collection as the Managed Object type and click Next.
 - **Note:** If you have installed other Netwrix change reporting products before, the list of Managed Object types may contain several options.

New Managed Object Select Managed Object Type	×
Installed Managed Object Types	
Computer Collection Get More	
Domain Organizational VMware Virtual Unit Center	
A computer collection can contain the following item types: EMC VNX/VNXe/Celerra, NetApp file: SDL Securitiestance: Suring Mindows File Security Mindows Security	
niei, og Loeiver instance, gyslog, windows file offale, windows betver.	
Previous Next Finish Cancel	

Figure 3: New Managed Object: Select Managed Object Type

- 4. On the **Specify Default Account** step, click the **Specify Account** button.
 - **Note:** If you have installed other Netwrix change reporting products before and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Account** and **Specify Email Settings** steps of the wizard will be omitted.

In the dialog that opens, enter the default Data Processing Account (in the domain_name\account_name format) that will be used by Netwrix Windows Server Change Reporter for data collection. This account must have the following rights:

- Local administrator rights on all monitored computers and on the computer where Netwrix Windows Server Change Reporter is installed (including the "Log on as a batch job" policy defined). For details, refer to Chapter 4 Configuring Rights and Permissions of <u>NetWrix Windows Server Change Reporter Installation and Configuration Guide</u>.
- If the computer with the product installed and the monitored servers belong to the same domain, this account must be assigned the domain administrator permissions.
- If the computer with the product installed and the monitored servers belong to workgroup or different domains, the target servers must have accounts with the same name and password as the account that is used for data collection. All these accounts must be assigned the local administrator permissions.
- All these accounts must be assigned the local administrator permissions, including the "Log on as a batch job" policy defined. For details, refer to Chapter 4 Configuring Rights and Permissions of <u>NetWrix Windows Server Change Reporter</u> Installation and Configuration Guide.
- If this account is going to be used to access the SQL database with audit data, it
 must also belong to the target database owner (dbo) role. For details on how to
 assign the dbo role to an account, refer to Chapter 4 Configuring Rights and
 Permissions of <u>NetWrix Windows Server Change Reporter Installation and
 Configuration Guide</u>.

New Manage	ed Object 🔀
	Specify Default Account
Userna	Lefault Data Processing Account
This acc you can	Specify the default Data Processing Account ed. n this
wizard.	User name: ENTERPRISE\administrator
	Password:
	Confirm password:
	, Note: This account must have the necessary rights and permissions to access your Managed Objects. More info: <u>Data Processing Account rights and permissions</u> .
	OK Cancel
	Previous Next Finish Cancel

Figure 4: New Managed Object: Specify Default Account

Click OK to continue and then Next.

- **Note:** If later you need to modify the default Data Processing Account, you can do this either for an individual Managed Object (for instructions, refer to <u>Procedure 3</u> <u>To modify the Data Processing Account</u>), or for all Managed Objects in a batch (for instructions, refer to <u>Procedure 22 To configure the Data Collection settings</u>).
- 5. On the **Specify Email Settings** step, provide the email settings that will be used for Change Summary and Reports delivery:

ew Mana	ged Object	
	Specify Email Settings	
Specify t	he email settings for Reports and Real-Time Alerts delivery.	
SMTP se	erver name:	
enterpris	se.loca	
Port: 2	25	
Sender a	address	
administ	rator@enterprise.local	Verifu
_		
🗆 SMT	PAuthentication	
SMT User	P Authentication rname:	
User	P Authentication : name:	
User	P Authentication rname: sword:	
SMT User Pass	P Authentication r name: word:	
SMT User Pass	P Authentication r name: word: implemented	
SMT User Pass Conf	P Authentication r name: sword: firm password:	
SMT User Pass Conf	P Authentication r name: sword: iim password:	
SMT User Pass Conf	P Authentication r name: sword: irm password: Secure Sockets Layer encrypted connection (SSL)	
SMT User Pass Conf	P Authentication r name: sword: irm password: Secure Sockets Layer encrypted connection (SSL) Irmilieit SSI: connection mode	
SMT User Pass Conf Use	P Authentication r name: sword: implessword: Secure Sockets Layer encrypted connection (SSL) Implicit SSL connection mode	
SMT User Pass Conf	P Authentication r name: sword: imp password: Secure Sockets Layer encrypted connection (SSL) Implicit SSL connection mode	
SMT User Pass Conf	P Authentication r name: sword: firm password: Secure Sockets Layer encrypted connection (SSL) Implicit SSL connection mode	
Conf	P Authentication r name: sword: iim password: Secure Sockets Layer encrypted connection (SSL) Implicit SSL connection mode	

Figure 5: New Managed Object: Specify Email Settings

The following parameters must be specified:

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

Table 2:Email Settings Parameters

Note: If later you need to modify the email settings, you can do this in **Settings** \rightarrow **Email Notifications** (for instructions, refer to <u>Procedure 20 To configure the email notifications settings</u>).

6. On the Specify Computer Collection Name step, enter your Managed Object name:

Figure 6: New Managed Object: Specify Computer Collection Name

New Manag	jed Object	×
	Specify Computer Collection Name	
Data P	Computer collection name: New Computer Collection	
Data i	TOCESSING ACCOUNT	
All ha:	operations with this Managed Object will be performed under this account. Make sure that it s the necessary rights and permissions.	
œ	Default (ENTERPRISE\administrator)	
	Note: If needed, you can change the default account later in Settings > Data Collection.	
0	Lustom User name: Password:	
	Previous Next Einish Cancel	

If you want to use a specific account to access components from this Computer Collection (other than the one you specified as the default Data Processing Account earlier in this procedure), select the **Custom** option and enter the credentials. This account must be granted the same permissions and access rights as the default Data Processing Account. Click **Next** to continue.

7. On the Add Modules step, make sure that the Windows Server Change Reporter module is selected under Installed Modules:

New Managed Object Add Modules Add Modules Select the modules you want to enable: Installed Modules Windows Server Change Reporter Image: I	righter i her managed object. Nad modules
Add Modules Select the modules you want to enable: Installed Modules Image: Select the modules of the select of the selec	ew Managed Object 🔰 🔰 🔁
Select the modules you want to enable: Installed Modules Is Windows Server Change Reporter Is User Activity Video Reporter Is Event Log Manager Is Event Log Manager Is SQL Server Change Reporter Is SQL Server Change Reporter Is Output Download Module	Add Modules
Installed Modules Image: Solution of the second s	Select the modules you want to enable:
Image: Solution of the second seco	Installed Modules
Download Module Click Update to receive an up-to-date list of available modules from NetWrix website.	E Windows Server Change Reporter Outright Server Change Reporter Outright Video Reporter Get More
Download Module Click Update to receive an up-to-date list of available modules from NetWrix website. Update	☐ 🚽 Event Log Manager ☐ 🚽 File Server Change Reporter ☐ 🚽 SQL Server Change Reporter
Download Module available modules from NetWrix website. Update	Click Undate to receive an unto-date list of
Previous Next Finish Cancel	Download Module Update to receive an up-to-date its to Update Update Previous Next Firrish Cancel

Figure 7: New Managed Object: Add Modules

Note: If you have not installed any other Netwrix change reporting products before, this step will be omitted.

On this step, under **Get More**, there is a list of other Netwrix products that can have Computer Collection as the Managed Object type. To get more information on these products and download them, select the corresponding checkbox, or click a module and then click **Yes**. You will be redirected to the product website page.

8. On the **Configure Reports Settings** step, select the **Enable Reports** checkbox if you want to use the SSRS-based Reports:

New Managed Object	×
Configure Reports Settings	
✓ Enable Reports	
Automatically install and configure a new instance of SQL Server Express Edition	
O Use an existing SQL Server instance with SQL Server Reporting Services	
SQL Server instance: WORKSTATION7\SQLExpress	
Vindows Authentication	
User name:	
Password:	
SQL Server Reporting Services	
Report Server URL:	
http://WORKSTATION7/ReportServer_SQLExpress	Verify
Report Manager URL:	
http://wORKSTATION7/Reports_SQLExpress	Verify
Previous Next Finish	Cancel

Figure 8: New Managed Object: Configure Reports Settings

Note: If you do not enable the **Reports** feature, audit data will not be written to a SQL database. If you wish to skip Reports configuration now, you can always enable and configure them later (for details, refer to Section <u>6.2 Configuring Reports</u> of this guide).

Select one of the following options:

- Automatically install and configure a new instance of SQL Server Express Edition to automatically install and configure SQL Server Express with Advanced Services. Once you have selected this option and clicked Next, the Reports Configuration wizard will start. Follow the instructions of the wizard to install and configure SQL Server Express. SQL Server version depends on the operating system your computer is running (for details, refer to the following Netwrix Knowledge Base article: Which SQL Server versions can be installed automatically via Netwrix Management Console).
- Use an existing SQL Server with SQL Reporting Services to use an already installed SQL Server instance, or to install and configure it manually before proceeding with the Netwrix Windows Server Change Reporter configuration. For detailed instructions on how to install Microsoft SQL Server 2005/2008 R2/2012 Express with Advanced Services and configure the Reporting Services, refer to the following Netwrix Technical Article: Installing Microsoft SQL Server and Configuring the Reporting Services.
- **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.

If you have selected the second option, specify the following parameters:

Parameter	Description
SQL Server instance	Specify the name of the SQL Server instance where a database of collected audit data will be created.
Windows Authentication	Select this option if you want to use the Data Processing Account specified earlier in this procedure to be used to access the SQL database.
User name	Specify a user name for the SQL Server authentication. NOTE: This user must belong to the target database owners (dbo) role. For instructions on how to assign this role to a user, refer to refer to Chapter 4 Configuring Rights and Permissions of <u>Netwrix Windows Server Change</u> <u>Reporter Installation and Configuration Guide</u> .
Password	Enter a password for the SQL Server authentication.
Report Server URL	Specify the Report Server URL. NOTE: It is recommended to press the Verify button to ensure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. NOTE: It is recommended to press the Verify button to ensure that the resource is reachable.

Table 3: Reports Parameters

Note: If you already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable the Reports feature. If you want to use custom Reports settings for this Managed Object (for example, write data to a different SQL database), you can change the

Reports settings later (for instructions, refer to Section <u>6.2.1 Specifying SQL Server</u> <u>Settings</u> of this guide).

Click **Next** to continue and wait until Netwrix Management Console has established a connection with the Report Server.

9. On the Add Items to Collection step, click Add to specify the computers you want to monitor:

New Manage	ed Object			×
	Add Items to Coll	ection		
Add comp	outers, shares, SQL Server	instances, and other	ritems to collection:	
Item		Source	Platform	Add
				Edit
				Bemove
				11011070
		1		
		Previous 1	Vext Finish	Cancel

Figure 9: New Managed Object: Add items to Collection

The Computer Collection New Item wizard starts.

10. On the Select Item Type step, select Windows Server as the item type, and click Next to specify the computers to monitor:

Figure 10: Computer Collection New Item: Select Item Type

Computer Collection New Item
Select Item Type
Select item type from the following list:
Item Types
Windows Server
Windows Server: a computer running Windows. You can add single computers, computers from within an Active Directory container or an IP range, or import of list of computers from a text file.
Brevious Next Einish Cancel

11. On the **Specify Items** step select one of the options and specify the computers to monitor.

nputer Collection New Item	
Specify Items	
Computer name:	
	Browse
Note: Enter the FQDN, NETBIOS or IP address.	
C Active Directory container:	
	Browse
Select the computer types you want to monitor:	
Domain controllers	
Servers (excluding domain controllers)	
☐ Workstations	
Exclude the computers you do not want to monitor	Exclude
IP address range:	
Start IP: 0.0.0.0 End IP: 0.0.0.0	Exclude
Import computer names from a file:	
()	Browse
Import once	
C Import on every data collection	
Province Next First	Cancel

Figure 11: Computer Collection New Item: Specify Items

- **Computer name** allows specifying a single computer by entering its FQDN, NETBIOS or IP address. You can click **Browse** to select a computer from the list of computers in your network.
- Active Directory container allows specifying a whole AD container. Click Browse to select from the list of containers in your network. Under this option you also can:
 - Select a particular computer type to be monitored within the chosen AD container: Domain controllers, Servers (excluding domain controllers), or Workstations. You can select more than one checkbox.
 - o Exclude the computers you do not want to monitor. To do this click **Exclude** to specify a container with the computers you do not want to monitor.
- **Note:** The list of containers does not include child domains of trusted domains. If the product is installed on a computer running Windows XP/2003, trusted domains will also not appear in the list of AD containers. Use a different choice option (Computer name, IP address range, or Import computer names from a file) to specify the target computers.
- IP address range allows specifying an IP range for the managed computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP range you want to exclude, and click **Add**:

xclude IP Address Ranges	;	×
Specify the sub-range(s) you	want to exclude:	
Start IP: 192.166.1.1	44 End IP: 192.166.1.	149 <u>A</u> dd
Start IP Address	End IP Address	<u>R</u> emove
132.160.1.120	132.166.1.130	
1		
	OK	Cancel

Figure 12: Exclude IP Address ranges

• Import computer names from a file allows specifying multiple computer names by importing a list from a .txt file (one computer name/IP address per line is accepted). You can choose whether to import the list once, or to update it on every data collection.

If you select the **Import on every data collection** option, you can later modify the list of your monitored computers by editing the .txt file. The monitored computers list will be updated on the next data collection.

Click Next to proceed and then Finish to complete the Add Items to Collection step.

12. On the Network Traffic Compression step you can enable the Network Traffic Compression option. If this feature is enabled, an agent will be installed automatically on the target servers that will collect and pre-filter data and return it in a highly compressed format. This significantly improves data transfer and minimizes the impact on target computers' performance.

New Managed Object 🛛 🗶
Network Traffic Compression
Enable Network Traffic Compression Network Traffic Compression is recommended for slow connections and/or distributed multi-site networks. When enabled, an agent is executed on each target computer collecting and compressing audit data before transfer. The program is executed on a schedule and completes quickly (in several minutes). This results in almost 100 times less data transferred with minimal impact on the target computer complet complet complet complet complet set formation.
the target computer performance.
Previous Next Finish Cancel

Figure 13: New Managed Object: Network Traffic Compression

13. On the **Configure Audit in Target Environment** step, select how you want to configure audit on your target computers: **Automatically** for the selected modules, or **Manually**.

Figure 14: New Managed Object: Configure Audit in Target Environment

New Managed Object	×
Configure Audit in Target Environment	
Successful change monitoring requires a certain configuration of the audit settings in your target environment. NetWrix modules can check your audit settings on each data collection and adjust them if needed. Select how you want to configure audit in the target environment.	
• Automatically for the selected modules:	1
✓ Windows Server Change Reporter	
C. Manually	
Refer to instructions on manual audit configuration.	
Previous Next Finish Cancel	

Note: Audit can only be configured automatically if the **Network Traffic Compression** option has been enabled on the previous step.

The following audit settings are configured automatically:

Parameter	Description
Windows Registry	Audit permissions "Set Value", "Create Subkey", "Delete", "Write DAC", and "Write Owner" are set to "Successful" for the following Windows Registry nodes: • HKEY_LOCAL_MACHINE\SOFTWARE • HKEY_LOCAL_MACHINE\SYSTEM • HKEY_USERS\.DEFAULT
	For pre-Vista Windows versions, the following policies are set to "Success":
	Audit object access
	Audit account management
Local Audit Policies	For Windows Vista and above, the following granular audit policies are set to "Success":
	 Account Management: Audit Security Group Management, Audit User Account Management
	 Object Access: Audit Registry, Audit Handle Manipulation, Audit Other Object Access Events
Event Log Size and Retention Method	The size of the Application, Security, System and Microsoft-Windows-TaskScheduler/Operational event logs is set to a maximum value:
	• for pre-Vista Windows version: 300 MB
	 for Windows Vista and above: 1 GB
	The retention method is set to "Overwrite events as needed".

Table 4: Audit Settings

Note: If your target computer is a domain controller, only the Windows registry audit permissions and the event log size with retention method can be configured automatically. Local audit policies need to be configured manually. For instructions on the manual audit configuration, refer to Chapter 5 Configuring Audit Settings on Target Servers of <u>Netwrix Windows Server Change Reporter Installation and Configuration Guide</u>.

Automatic audit configuration is performed on every data collection: the product checks the current audit settings and adjusts them to the values specified in <u>Table 4:</u> <u>Audit Settings</u> if they have been changed since the last data collection.

Click **Next** to continue.

- 14. On the Select Monitored System Components step, select the system components that you want to monitor for changes:
 - Figure 15: New Managed Object: Select Monitored System Components

New Managed Object			
s	elect Monitored System Con	nponents	
Enable	change auditing of the following syst	em components:	
V	General computer settings 🕕	Scheduled tasks	
	Hardware	Local users and groups	
	Add/remove programs	DNS configuration (1)	
	Services	DNS resource records (1)	
Windo	ws registry settings		
•	OS security	File sharing settings	
V	Security settings	USB devices	
V	Patches	Important services	
V	Windows Firewall	🗹 Startup and autorun	
	Remote Desktop	All other settings	
File an	d permission changes		
Learn more about file servers audit.			
Need to monitor changes to other system components? <u>Contact NetWrix Technical Support</u> .			
	Previous	Next Finish Cancel	

Note: For a full list of monitored components, refer to <u>A Appendix: Monitored</u> <u>Components and Settings</u>.

Click Next to continue.

15. On the Window Server Change Reporter Change Summary Delivery step, click the Add button to specify the Change Summary recipient(s):

ew Manag	ed Object E Windows Server Change Reporter Change Summary Delivery
Send Cł Name	nange Summary to: Add Edit
N	ew Email Address Specify a new email address: administrator@enterprise.loca OK Cancel
1	Previous Next Finish Cancel

Figure 16: Widows Server Change Reporter Change Summary Delivery

It is recommended to click the **Verify** button. The system will send a test message to the specified email address and will inform you if any problems are detected. Click **OK** to save the changes and then click **Next** to continue.

16. On the last step, review your Managed Object settings and click **Finish** to exit the wizard. A confirmation message will be displayed.

The newly created Managed Object will appear under the **Managed Objects** node, and its details will be displayed in the right pane:

File Action View Help Image: NetWrite Exterprise Management Console Image: Mindows Server Change Reports Image: Mindow Server Change Reports <tr< th=""></tr<>
Second Delacts Managed Items Managed Managed Managed Ma
Image: Console General Items Image: Console Items </th

Figure 17: Managed Object Page

4.2. Modifying Managed Object Settings

If later you need to modify the settings for an existing Managed Object, perform one of the following procedures:

- <u>To modify general settings</u>: add or remove Netwrix modules for the selected Managed Object.
- **Note:** This option is only available if you have already installed other Netwrix change reporting products that have Computer Collection as the managed object type.
- <u>To modify the Data Processing Account</u>: override the Default Data Processing Account for this Managed Object and specify a different account for data collection.
- <u>To add/remove items to/from Computer</u> Collection: add or remove items to/ from Computer Collection.
- <u>To modify Windows Server Change Reporter settings</u>: change the set of monitored system components, Change Summary recipients and enable/disable the product options.

Procedure 2. To modify general settings

- 1. In Netwrix Management Console, expand the **Managed Objects** node and select your Managed Object. The Managed Object page will be displayed showing a list of Netwrix modules added for this Managed Object.
- 2. Click the Add/Remove Modules button. A dialog containing a list of installed and available modules will be displayed:

Edit Managed Object		×
Add/Remove Mod	dules	
Select the modules you want to enable	e:	
Installed Modules		
Windows Server Change Re O User Activity Video Reporter Get More	porter	
Event Log Manager	r	
Download Module	Click Update to receive an up-to-date list of available modules from NetWrix website.	<u>U</u> pdate
	<u>Previous</u>	Cancel

Figure 18: Add/Remove Modules

3. To add other installed modules for this Managed Object, select them from the **Installed Modules** list and click **Next**. Follow the wizard to configure the selected modules for this Managed Object.

In this dialog, under **Get More**, there is also a list of other Netwrix products that can have Computer Collection as a Managed Object type. To get more information on

these products and download them, select the corresponding checkbox, or click a module and then click **OK**. You will be redirected to the product website page.

Procedure 3. To modify the Data Processing Account

- 1. In Netwrix Management Console, expand the Managed Objects node and select your Managed Object. Right-click it and select **Properties** from the popup menu.
- 2. In the dialog that opens, select the **Custom** option under **Data Processing Account** and specify the credentials:

rigule 17.	munuged Object Froperties	
Windows Computer Co	ollection Properties	×
Settings		
Name:	Windows Computer Collection	1
Data Processing A	Account	-
Default (ENTER	RPRISE\administrator)	
C Custom		
User name:		1
Password:		
	OK Cancel Apply	

Figure 19: Managed Object Properties

3. Click **OK** to save the changes. This account will be used for data collection from this Managed Object.

Procedure 4. To add/remove items to/from Computer Collection

- 1. In Netwrix Management Console, expand the Managed Objects node and select a Managed Object.
- 2. Click the **Managed Items** button, or switch to the **Items** tab. The following page will be displayed showing a list of monitored computers:

Figure 20: Managed Items

NetWrix Enterprise Management Conse	ole						_ 🗆 🗙
File Action View Help							
🗢 🔿 🗾 🖬							
Image: Part of the second	General Items	Arix tand Compliance naged Items - edit the collection shares, SQL Serve	Enterprise Ma	s to collection:	onsole	General Setting	s
	Item			Source	Platform	Add	. 1
	enterpriseDI			Computer	Windows Server	Edit	 IVE

- 3. Do one of the following:
 - <u>To add a computer</u>, click **Add** and follow the instructions of the **Computer Collection New Item** wizard (for details, see <u>Procedure 1 To create and configure</u> <u>a Managed Object</u>).
 - <u>To edit a computer name</u>, select a computer and click **Edit**. In the dialog that opens, modify the computer name and click **OK**.
 - <u>To remove a computer</u>, select it from the list and click **Remove**.

Procedure 5. To modify Windows Server Change Reporter settings

 In Netwrix Management Console, expand the Managed Objects → <Managed_Object_name> node and select Windows Server Change Reporter. The following page will be displayed:

NetWrix Enterprise Management Console		_ 🗆 🗵
File Action View Help		
🗢 🔿 📩 🖬 🛛 🖬		
File Action View Help Action View Help Image: Source Image: Source Image: Source Image: Managed Objects Image: Source Image: Source Image: Managed Objects Image: Source Image: Source Image: Mondows Computer Collection Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source Image: Source	Enclose E	
	Change Viewer Generate a Change Summary for a selected server Generate Summary	

Figure 21: Windows Server Change Reporter Page

- 2. To modify Netwrix Windows Server Change Reporter settings, do the following:
 - <u>To disable (or enable, if disabled) the Windows Server Change Reporter module</u> for this Managed Object, deselect/select the corresponding checkbox.
 - <u>To add an email address to the Change Summary recipients list</u>, click the Add button. Specify the email address and click OK. It is recommended to click the **Verify** button to validate this address. The system will send a test message and will inform you if any problems are detected.
 - <u>To modify an email address in the Change Summary recipients list</u>, select it and click the **Edit** button. Edit the address and click **OK**.
 - <u>To remove an email address from the Change Summary recipients list</u>, select it and click the **Remove** button. The selected address will be deleted.
 - <u>To disable (or enable, if disabled) the Network Traffic Compression option,</u> select/deselect the corresponding checkbox. It is recommended to enable this option, otherwise the collected audit data may be incomplete.
 - <u>To disable (or enable, if disabled) the Automatically configure audit settings on</u> <u>target servers option</u>, select/deselect the corresponding checkbox. For a list of the settings that will be configured automatically, refer to <u>Table 4: Audit Settings</u>.
 - <u>To modify the list of the system components you want to monitor</u>, click the Select Components button. In the Monitored System Components dialog, enable or disable the required checkboxes:

For a full list of the components and their settings monitored by Netwrix Windows Server Change Reporter, refer to <u>A Appendix: Monitored Components and Settings</u>.

5. DATA COLLECTION

This chapter provides a description of the data collection workflow, and the information on the Change Summary options and sessions.

This chapter covers:

- Data collection workflow
- <u>Change Summary</u>
- <u>Sessions</u>

5.1. Data Collection Workflow

Figure 22.

Netwrix Windows Server Change Reporter data collection workflow is as follows:

- 1. When a new Managed Object is created, Netwrix Windows Server Change Reporter starts collecting data from computers. The first data collection creates an initial snapshot of the monitored computers' current state. Netwrix Windows Server Change Reporter uses this information as a benchmark to collect data on changes made to the target computer collection. Each data collection is referred to as a Session.
- 2. After the initial analysis has been completed, an email notification is sent to the specified recipient(s) like in the example below:

Initial Analysis Natification

Figure 22.			
NetWrix Windows Server Change Repo	rter: Change Summary - Windows Computer Collection - Message (HTML)	- 0	×

a	ary - windows computer concention - message (i rime)	
File Message		∞ 😮
From: administrator@enterprise.local To: administrator@enterprise.local Cr:	Sent: Th	nu 4/4/2013 4:27 PM
Subject: NetWrix Windows Server Change Reporter: Change Summary - Windows Co	omputer Collection	
You are using the trial version of NetWrix Windows Server Change Reporter. The evaluation	on period expires in 19 days. <u>Click here to request a quote.</u>	
This is an automatically generated message sent from workstation7.enterprise.local.		
Change analysis completed successfully. No changes were detected on your server(s).		
You can modify the Change Summary delivery schedule in NetWrix Management Console	via Settings -> Data Collection	
Please visit www.netwrix.com for more products and updates.		
		_
		· · · · · · · · · · · · · · · · · · ·
See more about: administrator@enterprise.local.		· · ·

- 3. When the data collection has been completed, Netwrix Windows Server Change Reporter writes data on the detected changes to a local storage, the Audit Archive. By default, the data collection is performed once a day at 3:00 AM. If the Reports feature is enabled and configured, data is then imported from the Audit Archive to a SQL database.
- 4. At the same time, the product generates and emails a Change Summary to the specified recipients (for instructions on how to modify the Change Summary delivery schedule, refer to Section <u>7.4 Configuring Data Collection Settings</u>).
 - **Note:** For Netwrix Windows Server Change Reporter to be able to collect audit data successfully, you need to configure your monitored computers for audit prior to using the product. For detailed instructions on how to do this, refer to Chapter 5 Configuring Audit Settings on Target Servers of <u>Netwrix Windows Server Change Reporter Installation and Configuration Guide</u>.

5.2. Change Summary

Each day (at 3:00 AM by default), Netwrix Windows Server Change Reporter generates a Change Summary that contains the information on changes that occurred in the last 24 hours and emails it to the specified recipients:

		3999		NetWix Wind	lows Server Cl	ange Reporter: Change Si	ummary - Windows Computer Collection	Message (HTML)	- 0 - X-
		File	Message						∞ 0
		From: To: Cc Subject:	administrator Benterpris administrator Benterpris	e.local e.local Change Reporter: Ch	ange Summar	- Windows Computer Col	lection	Sent	: Fn 4/5/2013 4:34 PM
		You are usin This is an au	ig the trial version of NetW stomatically generated mes	rix Windows Server C sage sert from worl	hange Reports	r. The evaluation period ex	epires in 18 days. <u>Click here to request a qu</u> c	is.	122-4
	Administrator	Change ana	lysis completed successful	ly. The following char	ges were dete	cted on your server(s):			
		Change Type	Who Changed	When Changed	Server	Object Type	Resource Path	Details	
•	Uninstalls Adobe Flash	Removed	ENTERPRISE/Administrato	r 4/5/2013 4:55:52 Al	4 enterpriseD	C Add or Remove Program	is Add or Remove Programs\Adobe Flash Pl ayer 11 ActiveX (x64)	Object attributes: Version: "11.1.102.55" Installed For: "All uppers"	
	Payer 11 ActiveX	Modified	ENTERPRISE\Administrato	r 4/5/2013 4:56:21 A	M enterpriseD	C Computer Name	System Properties	Computer Description changed from "to ription"	"Computer Desc
•	Changes Computer name	Windows Added Removed Modified	Server Change Summar 0 1 1	•					
		Manu datai	ad encode at bits //	destation 7/Deposed	EQ1 Exercise				
		You can mo	dify the Change Summary d	elivery schedule in N	tWrix Manage	• ment Console via Settings	s -> Data Collection		
		Please visit	www.netwrix.com for more	products and update	s.				
									w.

Figure 23: Change Summary Example

The Change Summary provides the following information for each change:

Parameter	Description
Change Type	Shows the type of action that was performed on the monitored system component. The possible values are Added/Removed/Modified.
Who Changed	Shows the name of the account under which the change was made.
When Changed	Shows the exact time when the change was made.
Server	Shows the name of the server where the change was made.
Object Type	Shows the type of the system component that was changed, for example, "DNS Server".
Resource Path	Shows the path to the system component that was changed.
Details	Shows the before and after values for the modified component.

Table 5:Change Summary Fields

If required, you can <u>modify Change Summary delivery schedule</u> and <u>generate Change</u> <u>Summary on-demand</u>.

5.2.1. Generating Change Summary on Demand

If you wish to generate an on-demand Change Summary without waiting for a scheduled delivery, do the following:

Procedure 6. To generate Change Summary on Demand

1. In Netwrix Enterprise Management Console, navigate to Managed Objects \rightarrow <Managed_Object_name> (see Figure 17: Managed Object Page).

- 2. In the right pane, select **Windows Server Change Reporter** in the list of modules configured for the selected Managed Object, and click the **Run** button.
- 3. A Change Summary will be generated and sent to the specified recipient(s).

Note: Depending on the size of the monitored environement and the number of changes, Change Summary generation may take quite long.

5.2.2. Viewing Change Summary for the Specified Time Frame

If you wish to view the changes made to server configuration within some specified time frame, do the following:

Procedure 7. To View Change Summary for the Specified Time Frame

- 1. In Netwrix Enterprise Management Console, navigate to Managed Objects \rightarrow <Managed_Object_name> \rightarrow Windows Server Change Reporter (see Figure 21: Windows Server Change Reporter Page).
- 2. In the right pane, click the **Generate Summary** button next to **Change Viewer**. The Change Viewer tool will open:

		ws server change reporter vit
Change Viewer		×
This tool generate server over the spe	s a Change S cified time i	Summary for the selected Windows range.
Windows server:	enterprise	DC
From session:	4/10/2013	3 3:00:18 AM
To session:	 Next 	
	O This	4/11/2013 3:00:26 AM
		Generate Summary
		Close

Figure 24: Netwrix Windows Server Change Reporter Viewer

- 3. Select **Windows server** for which you would like to view the changes from the dropdown list.
- 4. Specify the time frame by selecting the sessions in the **From session** and **To session** drop-down lists.
- 5. Click the Generate Summary button.
- 6. You will be asked to save the result as an HTML document, to do that specify the file name and click **Save**.
- 7. The changes made to server configuration within the specified time frame will be displayed in a web browser:

C:\Us	ers\administrator.ENTERP	PRISE\Documents\Wi	indows Ser	ver Change Re	porter 10.0.0.151 5_22_2013 - Windows Internet Explorer	_ 🗆 🗡
00	🗢 🙋 C:\Users\administra	tor.ENTERPRISE\Docum	ents\Windov	vs Server Change	a Reporter 10.0.0.151 5_22_2013 6_03_39 AM - 5_22 💌 😽 🗙 🔽 Bing	P -
🔆 Favor	tes 🛛 👍 🙋 Suggested Si	ites 🔹 🧧 Web Slice Ga	allery 🔻			
€ C:\Us	ers\administrator.ENTERPRIS	E\Documents\Wind			🛅 + 🗟 - 🖻 🖶 + P	age + Safety + Tools + 🔞 +
The follo	ving changes were detected o	on your server(s):				
Change Type	Who Changed	When Changed	Server	Object Type	Resource Path	Details
Added	ENTERPRISE\Administrator	r 5/22/2013 6:03:23 AM	10.0.0.151	Add or Remove Programs	Add or Remove Programs\Skype™ 5.3	Object attributes: Version: "5.3.108" Installed For: "All users"
Modified	System	5/22/2013 6:03:39 AM	10.0.0.151	Registry Key	Registry\HKEY_LOCAL_MACHINE\system\CurrentControlSet\services\LanmanServer\Parameters	srvcomment (REG_S2) changed from "Computer 1" to "Computer Collection"
Modified	ENTERPRISE\Administrator	5/22/2013 6:03:39 AM	10.0.0.151	Computer Name	System Properties	Computer Description changed from "Computer 1" to "Computer Collection"
Windo	ws Server Change Summ	ary				
Added	1					
Remove	d 0					
Modifie	3					
View de	tailed reports at http://W	ORKSTATION7/Repo	orts SOLEx	press.		
		1-10			C-W	
YOU CAN	nodiry the Change Summary (delivery schedule in Netv	wrix Manage	ment Console via	Settings -> Data Lollection	
Please vi	sit <u>www.netwrix.com</u> for more	e products and updates.				
Done					🛛 🔹 👘 🖓 🛼 Computer Protected Mode: Off	🖓 🔹 🔍 100% 🔹 🏼

Figure 25: Change Summary for the Specified Time Frame

Note: Change Summary generation time depends on the selected date range and the size of the monitored environment, and can take quite long. It is recommended to use the <u>Reports</u> functionality to review changes made to the monitored domain.

5.3. Sessions

A session is a scheduled or on-demand data collection that triggers Change Summary generation and delivery. You can view sessions in two ways:

- <u>Under a particular Managed Object and particular Netwrix module enabled for it</u>: in Netwrix Management Console navigate to Managed Objects → <Managed_Object_name> Windows Server Change Reporter → Sessions.
- <u>In bulk for all Managed Objects and installed modules</u>: in Netwrix Management Console select the **All Sessions** node in the left pane.

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

🚽 NetWrix Enterprise Management Console					
File Action View Help					
🗢 🔿 📩 🖬 🔢 🖬					
 NetWrix Enterprise Management Console Managed Objects Mindows Computer Collection Mindows Server Change Reporter Subscriptions Subscriptions 2013.04.04 at 05:11120 AM, Thursday 2013.04.04 at 05:22:53 AM, Thursday 2013.04.05 at 30:052 AM, Triursday 2013.04.05 at 30:000 AM, Friday 2013.04.09 at 30:000 AM, Friday 2013.04.09 at 30:000 AM, Friday 2013.04.10 at 02:43:22 AM, Wednesday 2013.04.10 at 02:43:22 AM, Wednesday 	2013 Stat Sess	3.04.04 at 05:22:53 us: dule ion errors:	Enterprise Man	agement Console	
2013.04.10 at 03:00:10 Am, wearesday 2013.04.11 at 03:00:26 AM, Thursday Reports Final Notifications Audit Archive Data Collection Lucines O NetWrix Console Audit E Al Sessions	Win	dows server	Name enterpriseDC	Status Success	
	Serv	ver errors:	none		

Figure 26: Session Page

The following information is provided:

Table 6: Session Details

Parameter	Description
Status	Shows Session status. The possible values are Success and Error.
Module	Shows the NetWrix module that this Session is for.
Session errors	Displays an error text if the Session status is Error.
Windows server	Shows target computers' names.
Server errors	Shows an error text for each computer from the Windows sever list.

You can configure the number of Sessions available for review in Netwrix Management Console by specifying the date range for Sessions to be stored. For detailed instructions on how to do this, refer to Section <u>7.3 Configuring Audit Archive Settings</u>.

6. REPORTS

6.1. Reports Overview

Netwrix Windows Server Change Reporter allows generating reports based on Microsoft SQL Server Reporting Services (SSRS). The product provides a wide variety of predefined reports that will help you to stay compliant with various standards and regulations (SOX, HIPAA, FISMA, PC and many others). You can use different output formats for your reports, such as PDF, XLS, and so on.

Note: If your situation requires the use of additional report types, you can <u>order</u> <u>custom report templates</u> from Netwrix.

In Netwrix Windows Server Change Reporter, the following report types are available:

- <u>Overview</u>: This is a chart report that shows an overview of changes to Windows server configuration within the selected time frame. Four charts show data grouped by the monitored component, date, the user who made the changes, and the monitored Windows server. This is a drill-through report, which means that by clicking a chart you will be redirected to a report with the corresponding grouping of data that provides the next level of detail. For details, refer to Section <u>6.5</u> <u>Overview Report</u>.
- <u>Change Review History</u>: This is a report that shows all changes made to Windows server configuration. This report is an auxiliary tool that can be used in the basic change management process. For more details, refer to Section <u>6.6 Change Management</u>.
- <u>Change Reports</u>: Reports that provide data on changes made to the monitored server configuration components. These reports all have a different set of filters allowing you to manage the collected audit data in the most convenient way. The product provides many pre-defined report templates, covering the most important components of server configuration such as hardware and software, network services, security, and so on.

For a full list of available reports, expand the corresponding node under Managed Objects \rightarrow <Managed_Object_name> \rightarrow Windows Server Change Reporter \rightarrow Reports:

Figure 27: Reports

NetWrix Enterprise Management Console		_ 🗆 🗵
File Action View Help		
🗢 🔿 🔰 🖬 🚺 🖬		
	Reports Setting: Enterprise Management Console Available Reports	
Herricks and Software and Software Herricks evices Herricks evices Herricks evices Herricks evices Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorptoins Subcorpt		
	Configure Reports — Configure the Reports settings for Windows Server Change Reporter. Upload report tamplates from the product installation folder to the Report Server. Assign read access permissions to reports for specified users and groups. <u>View</u> reports in a web browser.	

6.2. Configuring Reports

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

- Specify SQL Server Settings
- Upload report templates to the Report Server
- Import audit data from the Audit Archive to a SQL database
- <u>Assign permissions to view web-based reports</u>

6.2.1. Specifying SQL Server Settings

If you have not enabled and configured the Reports feature on Managed Object creation, or if you want to modify the Reports settings for an existing Managed Object, do the following:

Procedure 8. To configure Reports

 In Netwrix Enterprise Management Console, expand the Managed Object → <Managed_Object_name> → Windows Server Change Reporter node and select Reports. The following page will be displayed: Figure 28: Reports Page

률 NetWrix Enterprise Management Console		
File Action View Help		
🗇 🔿 🗾 🖬		
Image: WetWrix: Enterprise Management Console Image: Wandows Computer Collection Image: Windows Server Change Reporter Image: Windows Server Change Reporter Image: Reports Image: Reports	Reports Settings NetWrix Enterprise Management Console Systems Merganet and Conducts Enterprise Management Console	
Change Management Hardware and Software	Available Reports	
Hardware and Software Network Services Overall Changes Subscriptions Subscriptions Subscriptions Mail Subscriptions Subscriptions Mail Aufi-Archive Audit Archive Audit Archive Audit Archive Netwirx Console Audit Al Sessions	Vierrieu This report shows an overview of changes to Windows servers in the selected time range (by default, the past week). Change Management Metwork Services Overal Changes System and Security	
	Configure Reports	-
	Configure the Reports settings for Windows Server Change Reporter.	
	Upload report templates from the product installation folder to the Report Server.	
	Assign read access permissions to reports for specified users and groups.	
	<u>View</u> reports in a web browser.	

2. Click **Configure** under **Configure Reports**, or switch to the **Settings** tab. The following page will be displayed:

Figure 29: Reports Settings

NetWrix Enterprise Management Console		. 🗆 🗙
File Action View Help		
🗢 🔿 🖄 📰 🛛 🖬		
Alt Sessions Alt Ses	Reports Settings Enterprise Management Console Reports Specify SQL and Report Server Settings Settings Specify SQL and Report Server Settings Image: SQL Server Connection Settings SQL Server Connection Settings Image: SQL Server Connection Settings Image: SQL Server Connection Settings Image: SQL Server Connection Settings Image: SQL Server Connection Settings Image: SQL Server Connection Settings Image: SQL Server SQLEXPRESS); Report Manager URL: http://work.staion?/Reports_SQLExpress; UMindows Costom SQL Server Server: SQL Server Server: Image: Server_SQLExpress Database: NetWrite_Windows_Server_Change_Reports Image: SQL Server Server: Image: Server_SqLExpress Image: SQL Server Database: NetWrite_Windows_Server_Change_Reports Image: SQL Reporting Services Report Server URL: Intp://work.staion?/ReportServer_SQLExpress Veridy SQL Report Manager URL: http://work.staion?/ReportServer_SQLExpress Veridy Database Retention Settings Image: SQLExpress Veridy Obstabase Retention Settings Image: SQLExpress Veridy Otabase Retention Settings	
	Apply	

3. Specify/modify the following parameters:

Parameter	Description			
Enable Reports	Select this checkbox to enable the Reports functionality for the selected Managed Object.			
Default	Select this option to use the default SQL Server connection settings.			
Custom	Select this option to specify your custom SQL Server connection settings.			
Server	Specify the name of an existing SQL Server instance where a database of audit data will be created.			
Database	Specify the SQL database name.			
User name	Specify the user to access the SQL Server. This user must belong to the target database owner (dbo) role. For details on how to assign the dbo role to an account, refer to Chapter 4 Configuring Rights and Permissions of <u>Netwrix Windows Server Change Reporter Installation</u> and Configuration Guide.			
Password	Specify the password to access the SQL Server.			
Windows Authentication	Select this option if you want to use the default Data Processing Account (specified on Managed Object creation) to access the SQL database. Deselect this option if you want to use the SQL Server authentication.			
Report Server URL	Specify the Report Server URL. NOTE: It is recommended to click the Verify button to ensure that the resource is reachable.			
Report Manager URL	Specify the Report Manager URL. NOTE : It is recommended to click the Verify button to ensure that the resource is reachable.			
Store audit data in the database for x days	Specify the retention period for audit data. Only the data for the specified period will be available in reports.			
	Click the Clear button if you want to delete all data from the SQL database.			
Clear all database entries	NOTE: The information on user access permissions is stored in the SQL database. Once you have used the Clear all database entries option, the data on access permission is deleted together with audit data. This may cause an error in the future when assigning users read access permissions. For instructions on how to resolve the issue, refer to the following Netwrix Knowledge Base Article: <u>Error: A transport-level</u> <u>error has occurred when sending the request to the server</u> .			

Table 7: Reports Settings

4. Click **Apply** to save the changes.

Note: If you skip Reports configuration on Managed Object creation and enable them later, you also need to do the following:

- <u>Upload the report templates to the Report Server</u> (if Reports are enabled on Managed Object creation, this operation is performed automatically). For details on how to upload report templates manually, refer to Section <u>6.2.2 Uploading Report Templates to the Report Server</u>.
- <u>Import audit data to the SQL database</u>. When you configure the Reports settings, an SQL database for audit data is created. If you skip Reports configuration on Managed Object creation, the database will not be created and audit data will only be written to the local repository, the Audit Archive. If later you enable the Reports feature for a selected Managed Object and want historical audit data to be available for reporting, you will have to import data from the Audit Archive to

the SQL database. For details on how to do this, refer to Section <u>6.2.3 Importing</u> <u>Audit Data to SQL Database</u>.

6.2.2. Uploading Report Templates to the Report Server

If you did not enable the Reports feature when creating a Managed Object, and decide to enable it later, you need to upload the report templates to the Report Server.

Procedure 9. To upload report templates to the Report Server

 On the Reports page (see <u>Figure 28: Reports Page</u>), click Upload under Web-based Reports. The system will upload the report templates to the Report Server and will display the following confirmation message when the operation is completed:

Figure 30:	Uploading Report Ter	nplates
Windows Server	Change Reporter	×
Configuring co	npleted succesfully.	
		Close

6.2.3. Importing Audit Data to SQL Database

If you did not enable the Reports feature when creating a Managed Object, and decide to enable it later, you may want to make audit data stored in the Audit Archive available for Reports. This can be done by importing data from the Audit Archive to a SQL database with the DB Importer tool. This tool can also be used for data recovery in case the database is corrupted.

Procedure 10. To import audit data

 Navigate to Start → All Programs → Netwrix → Windows Server Change Reporter → Advanced Tools and select DB Importer. The DB Importer dialog will open:

Figure	31:	Netw	rix DB Imp	orter	
🕞 NetWrix Windows 9	ierver Cha	nge Rep	orter DB Importe	r	×
This tool imports aud database. Select the t	lit data for ime range	the selec and click	ted Windows serve Import.	er to the SQL	
Managed object:		Window	s Computer Collec	tion	•
Windows server:		enterpris	eDC		•
From session:		4/27/201	.3 3:00:17 AM		•
To session:		4/28/201	.3 3:00:15 AM		•
Import audit data to:			Reporting Servi	ce Database	
Start import				Import	
				Close	

2. From the **Managed Object** drop-down list, select the Managed Object that you want to import audit data for.

- 3. From the **Windows Server** drop-down list, select the computer for which you want to import data.
- 4. Select the time range for which you want to import data from the **From session** and **To session** drop-down lists.
- 5. If you have not installed SQL Server, or you want to use a target database that differs from the one configured for this Managed Object to store historical audit data, click the **Reporting Services Database** button. The Report Configuration Wizard will be displayed:

Reports Configuration Wizard	
Select SQL Server Instance Source	
Install and configure a SQL Server instance	
Automatically download, install and configure Microsoft SQL Server 2012 Express Edition with Advanced Services on this computer.	
C Use an existing SQL Server instance	
Point to an existing SQL Server instance. SQL Server Reporting Services must be installed and configured for this server.	
Previous Next Finish Cancel	

Figure 32: Report Configuration Wizard

- 6. Select whether you want to create a new SQL Server instance, or use an exciting one, and then click **Next**. Follow the instructions of the wizard.
- 7. Verify the database settings and click OK.
- 8. Click the **Import** button to start importing data from the Audit Archive to the selected database. A confirmation message will be displayed on successful operation completion.

6.2.4. Assigning Permissions to View Reports

Your situation may require that different users in your organization have access to reports. By default, reports can only be accessed by domain administrators. To grant other users access to reports, do the following:

Procedure 11. To assign permissions to view reports

1. On the Reports page (see <u>Figure 28: Reports Page</u>), click Assign under Configure Reports. The following dialog will be displayed:
| SQL Database Access | allowed to access | the database: | E |
|---------------------|-------------------|---------------|---------------|
| Name | | | Add
Remove |
| | | | Close |

Figure 33: SQL Database Access

2. Click the Add button and specify the name of the user or group that you want to assign permissions to. You can click the 🗔 button to search for users or groups inside your Active Directory domain. Then click OK. The selected user(s) will now be able to view reports.

6.3. Viewing Reports

Netwrix Windows Server Change Reporter provides two options for viewing reports:

- In Netwrix Management Console
- In a web browser

6.3.1. Viewing Reports in Netwrix Management Console

Procedure 12. To view a report in Netwrix Management Console

- 1. In Netwrix Enterprise Management Console, navigate to Managed Objects \rightarrow <Managed_Object_name> \rightarrow Windows Server Change Reporter \rightarrow Reports.
- 2. Select a report from one of the folders. A page like the following will be displayed (report filters may vary depending on the selected report):

NetWrix Enterprise Management Lonsole			- 니 스
File Action View Help			
🗢 🔿 🔁 🖬 🛛 🖬			
Image: WetWrix Enterprise Management Console Image: Windows Computer Collection Image: Windows Server Change Reporter Image: Windows Server Change Reporter Image: Windows Server	Systeme Management and Compliance	Enterprise Management Console	
Change Management	Add or Remove Pro	grams	
Add or Remove Programs	This report shows all added or r	removed programs.	
Printers Changes English Retwork Services	Report Filters	View Report	
Overall Changes System and Security	Time frame:	Specific dates Subscribe	
Subscriptions Sessions	Sort By:	When Changed	
Settings All Sessions	From:	4/29/2013 12:33:27 AM	
	To:	4/30/2013 12:33:27 AM	
	What Changed:	%	
	Who Changed:	%	
	Where Changed:	*	

Figure 34: Add or Remove Programs Report Page

3. Specify the report filters and click the **View Report** button (**View Chart** for chart reports).

Note: A wildcard (%) can be used to replace any number of characters.

4. Wait for the report to be generated:

🚽 NetWrix Enterprise Management Console						_ 🗆 ×
File Action View Help						
(= =) 🖄 🖬 📓 🖬						
NetWrix Enterprise Management Console Managed Objects Managed Objects Mindows Computer Collection Windows Server Change Reporter Managed Server Change Reporter	Systems Management and	Complexee Entern	orise Managem	ent Console		
Charge Management Charge Management Ardware and Software Ardware and Software Hardware Charges Hardware Charges Mitters Charges Mitters Charges	Time frame: Si From: 4/ What Changed: 2/ Where Changed: 2/	pecific dates 💌	Sort By: To: Who Changed: Managed Object:	When Changed 5/1/2013 1:24:56 AM % Windows Computer Collection		ew Report ubscribe Close
General Changes System and Security	🔄 🔁 🚺 🛛 🖓 🚽	1 of 1 ▶ ▶ ←	o 🗟 🏼 🖓 🔲 🛍 🗖	• 100% •		
Subscriptions	4/30/2013 - Add o	r Remove Programs		NetWrix Win	dows Server Change Reporte	er
Setting Autor Setting Autor Setting Autor Autor Setting Autor Autor Setting Autor Autor Setting Autor Setting Autor Setting	Add or	Remove Pro	ograms			
All Sessions	Filter		Value			2
	From:		4/28/2013 1:24:56 A	uM		
	To:		5/1/2013 1:24:56 AM	4		
	Sort By:		When Changed			
	What Chang	od.	%			19
	Who Change	d:	96			
	Where Chan	aed:	96			
	Managed Ob	ject:	Windows Computer (Collection		1
	Where:	10.0.0.151				
	Action	Who Changed	When Change	d What Chan	ged	
	Removed	ENTERPRISE\Admin or	strat 4/30/2013 1	L:26:44 AM Add or Remo	ve Programs\Skype™ 5.3	
	Version	5.3.108"				
	Р	age 1 of 1		Nrix, and Compliance "	www.netwrix.com	

Figure 35: Add or Remove Programs Report (Console)

Chart reports provide a visual representation of the changes statistics on the monitored computers:

Figure 36: All Server Changes by User (Console)



6.3.2. Viewing Reports in Web Browser

To view a report in a web browser, do the following:

Procedure 13. To view a report in a web browser

1. Open a web browser and type the Report Server URL (you can find the URL in Netwrix Management Console by navigating to Settings \rightarrow Reports). Alternatively, in Netwrix Management Console, navigate to the Reports page (see Figure 28: Reports Page) and click View under Configure Reports. The following page will be displayed:



Figure 37: SQL Server Reporting Services Page

- **Note:** If you have other Netwrix change reporting modules installed, and if the Reports feature is enabled and configured for them, the SQL Server Reporting Services page will contain reports folders for all of these modules.
- 2. Click the Netwrix Windows Server Change Reporter folder and navigate to the report you want to generate. Click the report name. The report will be displayed showing the changes that occurred in the last 24 hours. On this page, you can specify filters to the selected report and click the View Report button (View Chart for chart reports) to apply them:

dd or Remove F	Programs - Repo	ort Manager -	Windows Int	ernet Explorer				
💽 🗢 🙋 htt	tp://workstation7/F	Reports_SQLEXF	PRESS/Pages/R	eport.aspx?ItemPath=	%2fNetWrix+Windows+	-Server+Change+Re 💌 💈	🗟 🐓 🗙 🔁 Bing	
avorites 🛛 👍 .	🥖 Suggested Site	es 👻 🩋 Web :	Slice Gallery 🔻					
Add or Remove Pr	rograms - Report M	lanager					🟠 • 🔊 - 🖃 🚔 •	Page + Safety + Tools •
ne > NetWrix \	Windows Server	Change Rep	orter > Hard	ware and Software	> Add or Remove P	rograms		Home Site Settings H
ne frame:	Specific dates			Sort By:	When Changed	•		View Report
	4/20/2012 2/2	7.29 AM		Tot	4/20/2012 2:27:20	-		
,,,,,,	14/23/2013 2.2	7720 MM		10.				
iat Changed:	%			Who Changed:	%			
iere Changed:	%			Managed Object:	%			
4 1 c	of 1 🕨 🕅	100%	•	Find Ne:	xt 🖳 🗸 😨 🖨	b 📒		
ument Map			4/30/2013 - /	Add or Remove P	rograms		NetWrix Windows Serv	ver Change Reporter
			Filter		Va	lue		
			Filter		Va	lue		
			From:		4/29	/2013 2:27:28 AM		
			Sort By		Whe	n Changed		
			What C	hanged:	%	in onlinged		
			Who C	nanged:	%			
			Where	Changed:	%			
			Manag	ed Object:	%			
			Wher	e: 10.0.0.1	151			
			Actio	on Who C	hanged	When Changed	What Changed	
			Remo In Ve	stalled For: All us ersion: 5.3.108"	PRISE\Administrato ers''	r 4/30/2013 1:26	i:44 AM Add or Remove Progr	ams\Skype™ 5.3

Figure 38: Add or Remove Programs Report (Web Browser)

6.4. Configuring Report Subscriptions

In Netwrix Windows Server Change Reporter, you can configure a Subscription to schedule automatic report generation and delivery. You can apply various filters to your reports, and select their output format. The report will be sent as an email attachment in the selected format:

🖂 🚽 🤊 🙂 🔶 🗇	I	
File Message		♡ ?
From: administ To: administ	trator @enterprise.local trator @enterprise.local	Sent: Tue 4/30/2013 2:18 PM
Subject: Windows	Server Change Reporter: Add or Remove Programs	
🖂 Message 📳 Add o	r Remove Programs (Add or Remove Programs).xls (16 KB)	
You have received this	message due to the following subscription:	
Subscription Name:	Add or Remove Programs	
Description:		
Report Name:	Add or Remove Programs	
Report Description:	This report shows all added or removed programs.	
The report is in the atta	ichment.	=
 See more about: 	administrator@enterprise.local.	

Figure 39: Report Delivered by Subscription

This section provides detailed instructions on how to:

- <u>Create a Subscription</u>
- Modify a Subscription
- Force on-demand report delivery

6.4.1. Creating a Subscription

To subscribe to a report, you must first upload the report template to the Report Server. Report templates are uploaded automatically when a report is generated for the first time. If you want to configure a subscription for a report you have not generated before, perform the procedure in Section <u>6.2.2 Uploading Report Templates to the Report Server</u>.

Procedure 14. To create a Subscription

 In Netwrix Management Console, navigate to Managed Objects → <Managed_Object_name> → Windows Server Change Reporter → Subscriptions. The following page will be displayed:

NetWrix Enterprise Management Console		
File Action View Help		
🗢 🔿 🞽 🖬 🚺 🖬		
Image: Nanagement Console Image: Objects Image: Objects	Enterprise Management Console Subscriptions The Subscriptions feature allows configuring automatic report generation and delivery.	
	Subscriptions:	Add Edit Remove

Figure 40: Subscriptions Page

- 2. Click the **Add** button to start the Report Subscription wizard. You can also start the Report Subscription wizard by selecting a report and clicking the **Subscribe** button on the report page.
- 3. On the Welcome page, click **Next**. When connection with the Report Server is established, the **Select Report** page will be displayed:

New Report Subscript	ion port	X
Subscription name: Description:	New Subscription	Ă
Report name: Report description:	Add or Remove Programs This report shows all added or removed programs.	•
		Y
	Previous Next Finish	Cancel

Figure 41: Select Report

4. Specify the following parameters and click **Next** to proceed:

Table 8:Subscription Settings

Parameter	Description
Subscription name	Specify the subscription name. This name will be displayed in Netwrix Management Console under the Subscriptions node.
Description	Enter the subscription description (optional).

Report name	Select the report that you want to subscribe to from the drop-down list. NOTE: If you start the Report Subscription wizard from a specific report, this field will be filled in automatically.
Report description	This field is filled in automatically depending on the selected report.

5. On the **Specify Report Recipients** step, click the **Add** button and specify the email address(es) of the report recipient(s). It is recommended to click the **Verify** button. The system will send a test message to the specified address and will inform you if any problems are detected. Click **OK** to add the address and then **Next** to proceed.

5 I), I I	
🔊 New Report Subscription	×
Specify Report Recipients	
Send report to:	
Name Add	
New Email Address	
Specify a new email address: administrator@enterprise.local	
Previous Next Finish Cancel	

Figure 42: Specify Report Recipients

6. On the **Specify Report Delivery Options and Filters** step, select the report delivery format (Excel/PDF/Word) and select the **Do not send empty reports** option if you do not want reports to be generated if no changes occurred during the reporting period. Specify the report filters (which differ depending on the selected report) and click **Next** to proceed.

New Report Subscription			×
Specify Repor	rt Delivery Opti	ons and Filters	
Report delivery format:		Excel	•
Do not send empty report	5		
Report Filters			
Sort By:		When Changed	•
What Changed:		%	
Who Changed:		%	
Where Changed:		14	_
	Previous	Next Einish Cano	sel

Figure 43: Specify Report Delivery Options and Filters

- 7. On the **Configure Report Delivery Schedule** step, specify the report delivery schedule. The following options are supported:
 - <u>Daily</u>: reports will be delivered at a specified interval (in days) at 3:00 AM.
 - <u>Weekly</u>: reports will be delivered on the specified day(s) of the week at 3:00 AM.
 - <u>Monthly</u>: reports will be delivered in the specified months on the selected date at 3:00 AM.
 - **Note:** The time specified is the local time on the computer where NetWrix Windows Server Change Reporter is installed.

rigure 44. Conjigure Report Derivery Schedule
New Report Subscription
Configure Report Delivery Schedule
Deliver reports: Daily Daily Schedule Weekly Every 1 = 08y(s)
Previous Next Finish Cancel

Figure 44: Configure Report Delivery Schedule

8. On the last step, review your Subscription settings and click **Finish**. The new Subscription will appear under the **Subscriptions** node in the left pane.

6.4.2. Modifying a Subscription

If later you need to modify an existing Subscription, perform the following procedure:

Procedure 15. To modify a Subscription

 In Netwrix Management Console, expand the Managed Objects → <Managed_Object_name> → Windows Server Change Reporter → Subscriptions node and select the Subscription you want to modify. The Subscription page will be displayed:

NetWrix Enternrise Management Console		
File Action View Help		
NetWrix Enterprise Management Console Managed Objects Managed Objects Mindows Server Change Reporter Mindows Server Reporter Mindows Serve	General Recipients Schedule Add or Remove Based on: Enable Description:	Enterprise Management Console e Programs /NetWrix Windows Server Change Reporter/Hardware and Software/Add or Remove Programs
	Report delivery form Do not send emp Report Filters Sort By: What Changed: Who Changed: Where Changed:	nat: Excel

Figure 45: Subscription Page

2. Modify the subscription parameters in the **General**, **Recipients** and **Schedule** tabs and click **Apply** to save the changes.

6.4.3. Forcing On-Demand Report Delivery

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

Procedure 16. To force on-demand report delivery

- In Netwrix Enterprise Management Console, expand the Managed Objects → <Managed_Object_name> → Windows Server Change Reporter → Subscriptions node and select the Subscription for the report that you want to generate and send now.
- 2. On the report Subscription page, click Run Now (see Figure 45: Subscription Page).

The report will be generated and sent to the specified recipient(s). The report will contain data starting from the last scheduled report delivery (or from Subscription creation time, if no scheduled deliveries have occurred so far) and until the last scheduled data collection time (3:00 AM by default).

6.5. Overview Report

Netwrix Windows Server Change Reporter provides a visual representation of all changes to the monitored computers in the Overview report.

The Overview report is comprised of four charts showing the changes made to the monitored computers grouped by the monitored component, date, the user who made the changes, and the monitored Windows server. Every chart has a drill-down functionality. When viewing this report you can navigate to the next level of details by clicking one of the segments in a chart.

Procedure 17. To view Overview Report

- In Netwrix Management Console, expand the Managed Objects → <Managed_Object_name> → Windows Server Change Reporter → Reports and select the Overview report.
- 2. Specify filters to the report and click the **View Report** button to apply them. The report will be displayed showing the changes made to Windows server configuration within the specified time frame:

NetWrix Enterprise Management Console				
e Action View Help				
🔿 🔼 🖬 🛛 🖬				
NetWrix Enterprise Management Console	NetWrix	Enterprise Manager	ment Console	
Managed Objects Managed Objects Managed Objects	Systems Management and Compliance	Enterprise manager		
🖃 🚦 Windows Server Change Reporter				
Reports Overview	Time frame:	Managed Object		1
🗉 🧰 Change Management	France Specific dates		windows compare conection	View Report
Changes with Video Hardware and Software	4/3U/2013 2:10:02 AM	iu. [5	5/7/2013 2:10:02 AM	Subscribe
🖭 🧱 Network Services				
Overall Changes System and Security				Close
 Subscriptions 	: 📰 🛐 🔤 🖣 1 of 1 🕨	H + 8 🖬 🖪 🖬 🖬	. ▼ 100% ▼	
🕀 📄 Sessions	5/7/2013 - Overview		NetWrix Windows Server Chang	ge Reporter
Settings				
All Sessions	Overview			
	This report shows an overview o	f changes to Windows servers in th	e selected time range (by default, the past week).	
	- 1.			
	Filter	Value		
	From:	4/30/2013 2:10:02	- AM	
	To:	5/7/2013 2:10:02 4	AM	
	Managed Object:	Windows Computer	r Collection	
	Changes by	Object Type	Changes by User	
			152	
	240			
	270 4			
			90	
	Add or Rep	nove Programs	ENTERPRISE\Administrator	
	Computer	State	ENTERPRISE\ENTERPRISEDC\$	
	Processor		Not applicable	
	Registry Ke	ey Tack	NT AUTHORITY\LOCAL SERVICE	
	System Se	rvice	system	
	Changes	by Date	Changes by Windows Server	
	250			
	250	241		
	월 200			
	e e			
	5 150			
	÷ 100		260	
	J 50			
	2 2 2	2 5 6		
	4/30/2013 5/2/201	3 5/4/2013 5/6/2013		
	5/1/2013	5/3/2013 5/5/2013		
		Date	10.0.0.151	
	Page 1 of 1	" " Net	Wrix, www.netwrix.com	

Figure 46: Overview Report

To get more information on the server configuration changes, click on a chart segment to drill down to the next level of detail. For example, by clicking a segment of the **Changes by User** chart you will see the detailed report on the changes made by the corresponding user.

NetWrix Enterprise Management Console					
File Action View Help					
🗢 🔿 🔁 💼 🛛 🖬					
NetWrix Enterprise Management Console Managed Objects Windows Computer Collection Monows Server Change Reporter Windows Computer Collection	NetWrix me Management and Compliance	Enterprise Manage	ement C	onsole	
Change Management Change Management Change with Video Change with Video Change with Video Change with Video Change Change Changes What Ch Change Support System and Security Managec Sessions	e: Specific dates 5/5/2013 2:10:02 AM anged: % hanged: % 10 Diject: Wrindows Computer C	Sort By: M To: Who Change Object Type: Collection	When Cha 5/7/2013 d: ENTERPR	anged 💽 2:10:02 AM IISE VAdministrator	View Report Subscribe Close
E O User Activity Video Reporter	4 4 1 of 1 ▶	H 🗧 🛛 🖉 🗐 🖬 🖬	🛃 🕶 🕴 100°	·6 •	
	3 - All Server Changes			NetWrix W	findows Server Change Reporter
7765 F Fil Frc To: Soi WH WH WH Ob Ma	report shows all server chan ter mm: rt By: nat Changed: no Changed: iere Changed: ject Type: naged Object:	rges filtered by date, server name 5/5/2013 2:10:02 5/7/2013 2:10:02 When Changed % ENTERPRISE\Adm % % Windows Comput	e and object (2 AM 2 AM 2 AM inistrator cer Collectio	n	
Act	ion Who Changed	When Changed	Where Changed	Object Type	What Changed
Add	ed ENTERPRISE \Administrat or	5/6/2013 7:05:00 AM	10.0.0.15 1	Add or Remove Programs	Add or Remove Programs\Skype™ 5.3
	ersion: "5.3.108"				
I	ion Who	When Changed	Whore	Object	What Changed
Att	Changed	Hinen Changea	Changed	Туре	And Changeu
Rem	oved ENTERPRISE \Administrat or	5/6/2013 8:25:14 AM	10.0.0.15 1	Add or Remove Programs	Add or Remove Programs\Skype™ 5.3
I	nstalled For: All users"				
	'ersion: 5.3.108"				
	Page 1 of 1		twri) diting and Complian	K, nce "	www.netwrix.com

Figure 47: Overview Report: Changes by User

6.6. Change Management

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

All server configuration changes detected by Netwrix Windows Server Change Reporter have the *New* status by default. If any of the changes seems to require an additional check regarding its validity, approval, and so on, you can set the status of the change to *In Review* and provide the reason for such status. Once the change has been approved or rolled back, you can set its status to *Resolved*.

6.6.1. Reviewing Changes to Windows Server Configuration

To be able to review changes and assign their statuses you need to open the *Change Review History* report in Netwrix Management Console or in a web browser.

Procedure 18. To review changes made to Windows server configuration

- In Netwrix Management Console, expand the Managed Objects → <Managed_Object_name> → Windows Server Change Reporter → Reports → Change Management node and select the Change Review History report.
- 2. Specify filters to the report and click the **View Report** button to apply them. The report will be displayed showing the changes made to Windows server configuration within the specified time frame:

NetWrix Enterprise Management Console							
File Action View Help							
2 📷 🛛 🖬							
NetWrix Enterprise Management Console	NotW	riv	Entororiso Manad	omont (oncolo		
Managed Objects	Systems Management and 0	Compliance	Enterprise Manag		UIBUIC		
Windows Compace Concentrial							
E 🖺 Reports							1
Change Management	Time frame: Spe	scific dates	Sort By:	When (Changed 🗾		View Repo
Change Review History	From: 4/2	9/2013 5:40:39 AM	1 Io:	4/30/2	013 5:40:39 AM		Subscribe
Marchard and Software	What Changed: 1%		Who Chang	ed: Enterpri	se\administrator		
Overall Changes Suctors and Security	Where Changed: 1%		Ubject Type	*			Close
Subscriptions	Heview Status: All		- Heason:	%			
E Sessions	Reviewed by: %		Managed Ol	oject: Windov	vs Computer Collec	tion	
All Sessions				-			
		of 1 🕨	H 4 🛛 🖉 🖽 🛄 💭] 🛃 🕶 100	% *		
	4/30/2013 - Change	3 Review Histo	iry		Network V	vindows Server Change i	керопег
	Chamme	Denter					
	Change	Review	v history				
	This is a second in a						
	allows reviewing t	port snows all ch these changes by	v setting their status and speci	fying the rea	/nere changed al son.	nd What changed values, and	
	E il te su		V-L				
	Filler		Value	20.444			
	To:		4/29/2013 3.40.	39 AM			
	Fort Buy		4/30/2013 3.40.	39 AM			
	What Change	d٠	%				
	Who Changed	u. 1.	Foterorise\admir	nistrator			
	Where Chang	ed:	%	100.000			
	Object Type:	cu.	%				
	Review Statu	s:	All				
	Reason:		%				
	Reviewed by:		%				
	Managed Obje	ert.	Windows Comp	ter Collectic	n		
	Planagea Obje		Windows compe	icer concelle			
	Review Status	- Now		Click to	undato statu	c	
	Reacon:	. Now	atvis	<u>enex ce</u>	apadee stata	2	
	Reviewed hy:	- Cent	JCy //	Undate	ed on:	_	
	Action	Who	When Changed	Where	Ohiect	What Changed	
	Action	Changed	When changed	Changed	Туре	What Changea	
	Removed	ENTERPRISE	4/30/2013 1:26:44 AM	10.0.0.15	Add or	Add or Remove	
		vauministrat or		T	kemove Programs	Programs\skype™ 5.3	
	Installed For	r: All users"					
	Version: 5.3	.108"					
	Pa	ge 1 of 1	u ⊒ ⊓Ne	twri	X,	www.netwrix.com	
			#1 for Change A	uditing and Complia	ince "		

Figure 48: Change Review History Report

3. Click the Click to update status link, select one of the statuses and provide your comments if required.

	1 igule 47.	Review Status	
eview St	atus		×
Select th	e review status and sp	pecify your reason.	
• New			
A nev	w change that has no	t been reviewed yet.	
🔿 In Re	view		
This	change has to be revi	ewed.	
O Reso	lved		
This	change has been revi	ewed and the issue is closed.	
Reason:			
			<u> </u>
			_1
I			
		OK Cancel	

Figure 49: **Review Status**

4. Click **OK** to save the changes. The **Review Status** and **Reason** fields will be updated with the information provided on the previous step

Review Status: In Review			<u>Click to</u>	update statu	<u>5</u>	
Rea	ason:	The	change is being checked.			
Re	viewed by	: ENTE	RPRISE\administrator	Update	d on:	4/30/2013 6:34:26 AM
Act	tion	Who Changed	When Changed	Where Changed	Object Type	What Changed
Ren	noved	ENTERPRISE \Administrat or	4/30/2013 1:26:44 AM	10.0.0.15 1	Add or Remove Programs	Add or Remove Programs\Skype™ 5.3
Installed For: All users"						
١	Version: 5.	3.108"				

Figure 50:	Updated Review Status
------------	-----------------------

Note: If you are updating the status of a change in a web browser, you can specify as much information in the comments field as required, however, if the text contains more than 150 characters, you will not be able to change the status for this change once again. Provide long descriptions only for those changes for which you do not plan to change the status in the future.

7. CONFIGURING GLOBAL SETTINGS

Netwrix Management Console provides a convenient interface for configuring or modifying the settings that will be applied to *all* existing Managed Objects and *all* Netwrix modules enabled for these objects. This chapter provides detailed instructions on how to configure these settings.

Note: For instructions on how to configure or modify the settings for an individual Managed Object, or a Netwrix change reporting module enabled for this object, refer to Section <u>4.2 Modifying Managed Object Settings</u>.

To access global settings, expand the Settings node in the left pane:

📝 NetWrix Enterprise Management Cons	ole	
File Action View Help		
🗢 🔿 🖄 🖬 🚺 🖬		
 NetWrix Enterprise Management Console Managed Objects Windows Computer Collection Settings Reports Email Notifications Audt Archive Data Collection Licenses NetWrix Console Audit All Sessions 	Image: Settings Enterprise Management Console Image: Settings Common settings applied to all Managed Objects and all installed modules. Image: Settings Common settings applied to all Managed Objects and all installed modules. Image: Settings SqL Server and Report Server settings. Image: Settings SqL Server and Report Server settings. Image: Settings SMTP server settings for email delivery. Image: Setting: Settings Audit Archive Image: Audit Archive location and retention settings. Settings Image: Setting: Setting Setting: Setting Seting Setting Setting Setting Seting Setting S	

Figure 51: Settings Page

The following global settings can be configured:

- <u>Reports settings</u>
- Email Notifications settings
- <u>Audit Archive settings</u>
- Data Collection settings
- Licenses settings
- <u>Netwrix Console Audit</u>

7.1. Configuring the Reports Settings

The **Reports** option allows configuring the SQL Server and Report Server settings. To configure these settings, or modify your existing Reports settings, do the following:

Procedure 19. To configure the Reports settings

1. In Netwrix Management Console, expand the **Settings** node and select the **Reports** node. Alternatively, you can click **Reports** in the **Settings** page. The following page will be displayed showing the current Reports settings:

NetWrix Enterprise Management Console		
File Action View Help		
🗢 🤿 🖄 📰 🛛 🖬		
NetWrix Enterprise Management Console Managed Objects Mindows Computer Collection E Windows Server Change Reporter	Enterprise Management Console	
Reports Subscriptions	Reports Settings	
	Default SQL Server and Report Server settings	
Email Notifications	Reports Enabled: yes	
Audit Archive	SQL Server instance: WORKSTATION7\SQLExpress	
Licenses NetWrix Console Audit	SQL Server Reporting Services	
All Sessions	Report Server URL: <u>http://WORKSTATION7/ReportServer_SQLExpress</u>	
	Report Manager URL: <u>http://WORKSTATION7/Reports_SOLExpress</u>	
	Configure Reports settings	
	Apply Reports settings to all Managed Objects	

Figure 52: Settings: Reports

2. Click **Configure** in the right pane. The following dialog will be displayed:

Figure 53: Reports Settings

Configure Reports Settings	×
✓ Enable Reports	
SQL Server instance: WORKSTATION7\SQLExpress	
Vindows authentication	
User name:	
Password:	
SQL Server Reporting Services	_
Report Server URL: http://wORKSTATION7/ReportServer_SQLExpi Verify	
Report Manager URL: http://WORKSTATION7/Reports_SQLExpress Verify Note: parameter is optional	
Start the Reports Configuration wizard to install SQL Server, configure the Reporting Services and create an audit database.	
OK Cancel	

3. Modify your current reports settings if necessary and click **OK** to save the changes. For a detailed explanation of the reports parameters, refer to <u>Table 3: Reports</u> <u>Parameters</u>.

7.2. Configuring the Email Notifications Settings

The **Email Notifications** option allows configuring the SMTP settings used to deliver Change Summaries and Reports. To configure these settings or modify your existing email delivery settings do the following:

Procedure 20. To configure the email notifications settings

1. In Netwrix Management Console, expand the **Settings** node and select **Email Notifications**. Alternatively, you can click **Email Notifications** in the Settings page. The following page will be displayed showing the current email settings:

Elle Action View Help	
A dS essions A dS essions A ddf Archive A ddf	

Figure 54: Settings: Email Notifications

2. Click the Modify button in the right pane. The SMTP Settings dialog will be displayed:

Figure 55: SMTP Settings
SMTP Settings
Specify the default email delivery settings.
SMTP server name:
enterprise.local
Port: 25
Sender address:
administrator@enterprise.local Verify
I SMTP Authentication
User name:
Password:
Confirm password:
Use Secure Sockets Layer encrypted connection (SSL)
Implicit SSL connection mode
OK Cancel

 Modify you current email settings if necessary and click OK to save the changes. For a detailed explanation of the email parameters, refer to <u>Table 2: Email Settings</u> <u>Parameters</u>.

7.3. Configuring Audit Archive Settings

The **Audit Archive** option allows configuring location and retention period for the local repository of audit data. To configure these settings, do the following:

Procedure 21. To configure the Audit Archive settings

1. In Netwrix Management Console, expand the **Settings** node and select the **Audit Archive** option. Alternatively, you can click **Audit Archive** in the Settings page. The following page will be displayed showing the current Audit Archive settings:

NetWrix Enterprise Management Console		
File Action View Help		
🗢 🔿 🙍 🖬		
Id [®] NetWrix Enterprise Management Console	Enterprise Management Console Image: Audit Archive Audit Archive is a local file-based storage of audit data. Image: Write data to the Audit Archive Write audit data to: Image: CVProgramData/NetWirk/Management Console/Data Specify the retention period for sudit data (in months): Image: Specify the retention period for Sessions (in days):	Browse
		Apply

Figure 56: Settings: Audit Archive

2. Modify the following settings if necessary:

Parameter	Description
Write data to the Audit Archive	Enable this checkbox to be able to store audit data for a longer period.
Write audit data to	Specify the path to the folder where your audit data will be stored. Click the Browse button to select a location.
Specify the retention period for audit data (in months)	Specify the number of months for which audit data will be stored. Data will be deleted automatically when its retention period is over. If the Write data to the Audit Archive option is disabled, or the retention period is set to 0, data will be stored for the last 2 sessions.
Specify the retention period for Sessions (in days)	Specify the number of days for which Sessions (i.e. the information on daily data collection status) are stored and are available for review in Netwrix Management Console. NOTE: The Session retention period does not affect the Audit Archive retention setting.

Table 9:Audit Archive Settings

Note: It is strongly recommended not to disable the **Write data to the Audit Archive** option, since if audit data is not written locally, it will not be imported to the SQL database and will be unavailable for reports.

7.4. Configuring Data Collection Settings

The **Data Collection** option allows modifying the default schedule for data collection and Change Summary generation and delivery, as well as the default Data Processing Account.

Procedure 22. To configure the Data Collection settings

1. In Netwrix Management Console, expand the **Settings** node and select the **Data Collection** option. Alternatively, you can click **Data Collection** in the Settings page. The following page will be displayed showing the current data processing settings:

Netwrix Enterprise Management Console		_ U ×
File Action View Help		
🗢 🔿 🖄 📧 🛛 🖬		
NetWrix Enterprise Management Console Managed Objects Mindows Computer Collection Mindows Server Change Percenter	Enterprise Management Console	
Constructions Construction Construction	Data Collection Settings	-
Settings Reports Email Notifications	Data Collection and Change Summary Generation Schedule: At 300 AM every day, starting 4/23/2013 Modify	
Audit Archive Audit Archive Licenses NetWrix Console Audit All Sessions		
	Default Data Processing Account	_
	User name: ENTERPRISE\administrator Modify	

Figure 57: Settings: Data Collection

2. Click the Modify button next to Data Collection and Change Summary Generation Schedule.

3. In the **Delivery Schedule** dialog, specify a new time and frequency for the data collection:

Delivery Cale adul

Figure 58: Delivery Schedule	
Delivery Schedule	? ×
Schedule	
At 3:00 AM every day, starting 4/29/2013	
Schedule Task: Start time: Daily I 3:00 AM Advanced	
Schedule Task Daily	
Every 1 day(s)	
Show multiple schedules.	
	ancel

F:---- FO.

4. To access the advanced schedule options, click the **Advanced** button, and select the required options:

Figure 59: Advanced Schedule Options

Advanced Schedule Optio	ns			? ×
Start Date:	Tuesday ,	April	30, 2013	•
🔽 End Date:	Wednesday,	May	15, 2013	•
✓ Repeat task Every: 10 Until: C ✓ Duration: [✓ If the task is	minutes	r(s)	minul time.	te(s)
		OK	Canc	el

- 5. Click **OK** to apply the changes and close the dialog.
- 6. To specify a different account for data collection and processing, click the **Modify** button next to the **Default Data Processing Account** option.
- 7. In the **Default Data Processing Account** dialog, enter the account name, and password, and click **OK**:

	,	-
Defa	ult Data Processing Account	×
8	Specify the default Data Processing Account	
<u>U</u> ser na	ame:	
ENTER	RPRISE\administrator	
<u>P</u> asswo	ord:	
••••		
<u>C</u> onfin	m password:	
••••		
Note: T to acce More ir	his account must have the necessary rights and pe ss your Managed Objects. nfo: <u>Data Processing Account rights and permissior</u>	rmissions <u>15</u> .
_		
	ОК	Cancel

Note: Ensure that the new account has the required rights to collect data from the monitored computers. For more details, refer to Chapter 4 Configuring Rights and Permissions of <u>Netwrix Windows Server Change Repoter Installation and Configuration Guide</u>.

Default Data Processing Account

7.5. Configuring License Settings

Figure 60:

The **Licenses** option allows viewing your current licenses for the installed Netwrix products, updating them, and adding new licenses. To configure your licenses, perform the following procedure:

Procedure 23. To configure licenses

1. In Netwrix Management Console, expand the **Settings** node and select the **Licenses** option. Alternatively, you can click **Licenses** in the Settings page. The following page will be displayed showing the list of your current licenses:

The first find the first									
File Action View Help									
🗢 🔿 🙍 🖬 🛛 🖬									
Intervise Management Console Image of Objects Managed Objects Windows Computer Collection Image of Objects Windows Server Change Reporter Settings Reports Reports Image Networks Image Networks Image Network Ima	Systems Ma	etWri nagement and Compi Licenses The table be	Iow lists your current licenses fo	Nanag r all installe	ement Co	nsole			
Data Collection		Compan	Module	License	License Expires	Maintenance Expires	Licensed Am	Actual Am	
Licenses NetWrix Console Audit		VetWrix	Windows Server Change Reporter	Enterprise	5/31/2013	5/31/2013	100 computers	1 computers	
 ☑ NetWrix Console Audit ☑ ▲ All Sessions 		Add/Updat	e Remove r NetWrix Sales Representative fo	or any detai	ils on licensing.				

Figure 61: Settings: Licenses

2. Perform one of the following operations if necessary:

- <u>To add/update your licenses</u>, click the **Add/Update** button. In the dialog that opens, specify your company name, your license count and the license codes (separated by commas or semi-colons).
- **Note:** You can only add multiple licenses at the same time if they have the same license count. Otherwise, add them separately.
- <u>To remove a license</u>, select it from the list and click the **Remove** button. Then click **Yes** in the confirmation dialog.

7.6. Configuring Netwrix Console Audit

The Netwrix Console Audit option allows auditing changes made via Netwrix Management Console. This option is available if you have installed the Netwrix User Activity Video Reporter module. This tool captures video of any activity on the monitored computer and embeds metadata (such as the information on which applications and windows were opened) into video files, which can be used for data search and positioning inside video recordings. By configuring Netwrix User Activity Video Reporter to monitor Netwrix Management Console you can keep record of any actions performed using Netwrix Management Console and track changes to Netwrix modules configuration, Managed Objects and global settings.

Procedure 24. To enable Netwrix Console Audit

1. In Netwrix Management Console, expand the **Settings** node and select the **Netwrix Console Audit** option. Alternatively, you can click **Netwrix Console Audit** in the Settings page. The following page will be displayed:

NetWrix Enterprise Management Console		×
File Action View Help		
🗇 🔿 🔀 📊 🛂 🗊		
NetWrix Enterprise Management Console Managed Objects Mindows Computer Collection Mindows Server Change Reporter	Enterprise Management Console	
Settings Reports	Ready to configure audit	
Enal Notifications Audit Archive Deta Collection Lecreses Methy Lecrese Methy Console Audit All Sessions	NetWrix Console Audit Tracking of changes to NetWrix modules configuration, Managed Objects and global settings. Click "Configure" to automatically create a Managed Object with predefined settings for video tracking of changes to NetWrix Management Console. Configure	

Figure 62: Settings: Netwrix Console Audit

2. Click **Configure** to enable Netwrix Console Audit. A Managed Object will be created automatically with the following default settings:

Table 10:	Managed Object Default Settings
-----------	---------------------------------

Parameter	Status
Enabled module	User Activity Video Reporter
Monitored computers	localhost
Video recording filters by user	All users

Video recording filters by application	Netwrix*
SSRS-based Reports	Not configured
Automatic Activity Summary delivery	Not configured
Video recording quality and duration settings	Default

3. Click **OK** when the confirmation message is displayed. The newly created Managed Object will appear under the **Managed Objects** node, and the status of Netwrix Console Audit will change to "On":



Figure 63: Settings: Enabled Netwrix Console Audit

Once you have enabled the **Netwrix Console Audit** option, you will receive **Activity Summaries** with a list of video recordings and links to video files showing how the changes were made. By default, Activity Summary is generated and sent every hour starting from 7:00 AM:

FIGULE 04: ACLIVILY SUITH	nary
---------------------------	------

	1.0	15 4 3	-	NetWriv Use	er Activity Video Reporter: Acti	vity Summany – NetWrix Co	nsole Audit - Message (HTML)	- • X
		0	•	1000	. Activity video reporten Acti	ing summary inclume co	nsole Addie Micssage (TTME)	
File	2	Message						♥ 🕜
🚯 If	If there are problems with how this message is displayed, click here to view it in a web browser.							
From		🗌 administ	rator@enterp	orise.local			Sent:	Wed 5/1/2013 5:01 PM
To:	o: administrator@enterprise.local							
CC	et.	Not Aria LL	or Activity V	idaa Banad	tor Artivity Cummon MatMriv	Concolo Audit		
Subje	u.	Netwink O:	Sel Activity v	Ideo Kepon	ter: Activity Summary – Netvyrix	Console Addit		
You	are usi	ing the trial v	ersion of Ne	tWrix User /	Activity Video Reporter. The eva	aluation period expires in 20	days. <u>Click here to request a quote.</u>	[2]
This	s is an a	utomatically	generated n	nessage ser	t from WORKSTATION7 acco	rding to the following delive	ry setting for NetWrix Console Audit comput	ter collection: send
Act	ivity Su	mmary every	1 hour.					
The	table h	elow shows i	user activity	records car	tured since the last Activity Su	mmary delivery. To watch a v	ideo, download and install the codec	
				recordo cap	carea onice che hoe ricerney ba	initiary dentery to nater a t	deo, <u>comioso ano motar die codeci</u>	
Clic	k the "S	start time" link	to play a v	ideo.				
_								
Da	ate	Start time	End time	Duration	Computer	User		
5/	1/2013	4:53 AM	5:04 AM	00:10:54	workstation7.enterprise.local	ENTERPRISE\administrator		
То	madific	the Activity C	ummanı dali	ven interve	Latart NatWriv Management C	anala and paviasta to Mana	and Objects -> NotWriv Consola Audit -> Upor	Activity Video
Rep	orter. (On the right, o	lick the Con	figure butto	n for Email Notifications and se	et a new value for the deliver	y interval.	Activity video
Please visit www.netwriv.com for more products and updates								
	rease that <u>intranset interproducts</u> and optical.							
0	Sec	more about	administrat	or@enterpri	se local			2
	U See more about, auministrator wenterprise accar.							

You can generate a summary of activity records made for your console and Managed Object configuration changes via the Activity Records page by navigating to Managed Objects \rightarrow <your Managed_Object_name> \rightarrow User Activity Video Reporter \rightarrow Activity Records.

You can modify the Netwrix Console Audit settings (for example, enable SSRS-based Reports, subscribe to a report, and so on) in the same way as for any other Managed Object.

For details on the User Activity Video Reporter module functionality, refer to the <u>NetWrix</u> <u>User Activity Video Reporter Administrator's Guide</u>.

8. ADDITIONAL CONFIGURATION

This chapter provides instructions on how to fine-tune Netwrix Windows Server Change Reporter using the additional configuration options. It explains how to:

- Configure integration with Netwrix User Activity Video Reporter
- Exclude or include data types from/ in reports

8.1. Configuring Integration with Netwrix User Activity Video Reporter

By integrating Netwrix Windows Server Change Reporter with Netwrix User Activity Video Reporter, you can get a report that shows all changes made to Windows server configuration with links to the corresponding video files showing *how* a particular change was made.

Once the integration has completed, the **Changes with Video** subfolder containing the **All Changes with video report** will be added to the **Report** folder of the Netwrix Windows Server Change Reporter module.

Integration can be enabled if the following conditions are met:

- The Netwrix User Activity Video Reporter module is enabled and configured for the same Managed Object as Windows Server Change Reporter. For details on how to configure the module, refer to <u>Netwrix User Activity Video Reporter Administrator's Guide</u>.
- SSRS-based Reports are enabled and configured for both Netwrix Windows Server Change Reporter and Netwrix User Activity Video Reporter.
- Both the Windows Server Change Reporter and User Activity Video Reporter modules are configured to use the same SQL Server instance. You can check the SQL Server instance settings for each Managed Object in the <Managed Object name> → Windows Server Change Reporter/ User Activity Video Recorder → Reports → Settings page.
- At least one data collection must run on your Managed Object by Netwrix Windows Server Change Reporter. For details on how to run data collection, refer to Section <u>5.2.1 Generating Change Summary on Demand</u>.

Procedure 25. To enable integration with Netwrix User Activity Video Reporter

- 1. In the Netwrix Management Console tree, navigate to Managed Objects \rightarrow <Managed_Object_name> \rightarrow User Activity Video Reporter.
- 2. Click the Integrate video records link at the bottom of the User Activity Video Reporter main page:

RetWrix Enterprise Management Console				
File Action View Help				
🗢 🔿 🙍 🖬 🛛 🖬				
NetWrix Enterprise Management: Console Managed Objects Managed Objects Managed Discus Managed Discus Mindows Computer Collection Media Server Change Reporter Windows Server Change Reporter Settings Reports Settings Reports Multi Archive Audit Archive Obta Collection Utenses Media Vertice Audit Ald Sessions	Enterprise Management Console User Activity Video Reporter Automatic screen video capture and reporting on monitored users' activity. Enable User Activity Video Reporter Users			
	Specify Users			
	Specify the applications you want to track Video Recording Settings			
	Configure video recording quality, duration, and retention settings Configure Video			
[Configure Activity Summary delivery settings Configure Delivery			

Figure 65: User Activity Video Reporter Page

3. In the Integrate Video Records dialog, select Windows Server Change Reporter from the list and click the Integrate button:

Figure 66: Integrate Video Records

Windows S	erver Change Reporter	Managed Object Windows Computer Collec	Status Integrated	
	User Activity Video Rep	oorter	×	
Integration successful. R to reports with integrate		estart NetWrix Management Consol 1 video records.	e to get access	
			ОК	
Integrate				

- 4. If the operation is completed successfully, the status of the selected module changes to "Integrated". If it fails, a message is displayed explaining the reason why integration has failed.
- 5. Restart Netwrix Management Console for the changes to take effect.

The report with videos on the changes made to your target computers is available in the **Changes with Video** folder under the **Reports** node of the relevant Managed Object:

NetWrix Enterprise Management Console	🗖 Net Wrix Enterprise Management Console					
File Action View Help						
🗢 🔿 🗾 🖬 🛛 🖬						
NetWrix Enterprise Management Console Managed Objects Managed Objects Managed Objects Managed Objects Managed Console Audit @ User Activity Video Reporter @ Verview @ Change Management @ Overview @ Changes with Video @ Hardware and Software @ Overall Changes @ Overall Changes @ Overall Changes @ Subscriptions @ Subscriptions @ Subscriptions @ Essions @ Ethings @ Reports @ End Notifications Mud Video @ Audit Archive @ Data Collection Putrix Console Audit @ All Sessions	Enterprise Management Console Available Reports All Changes with video This report shows all changes with a link to a video record made by NetWrix User Activity	ty Video Reporter.				

Figure 67: Reports: Changes With Video

This report contains an additional column called "Video" which contains links to the corresponding video files showing *how* each change was made:

률 NetWrix Enterprise Management Console							_ 🗆 ×
File Action View Help							
🗢 🔿 🗡 📧 🛛 🖬							
Image: Instant Console Image: Imag	Systems Management	and Compliance	Enterprise Mana	ngement C	onsole		
Overview Change Management Changes with Video Martichanges with video Martichanges with video Martichanges Overall Changes System and Security Subscriptions	Time frame: From: What Changed: Where Changed: Show changes with only:	Specific da 5/6/2013 6 % % Yates	tes v k20:21 AM III	Sort By: To: Who Changed: Object Type:	When Changed 5/7/2013 8:35:21 %		View Report Subscribe Close
	: III 1 14 4	1 of 1 🕨	H ♦ 3 2 ∄ 🔳) 💭 🛃 🗸 📋 100'	% •		
Settings	5/6/2013 - All Ch	anges With Vid	eo		Net	Wrix User Activity Vide	eo Reporter
	All Cha	anges W	/Ith VIdeo h a link to a video record m	ade by NetWrix U	ser Activity Vide	o Reporter.	
	Filter		Value				
	From:		5/6/2013 8:2	U:21 AM			
	To:		5/7/2013 8:3	5:21 AM			
	Sort By:		When Chang	ed			
	What Chan	ged:	%				
	Who Chang	ed:	%				
	Where Cha	nged:	%				
	Object Typ	e:	%				
	Show chan	ges with video	only: Yes				
	Action	Who Changed	When Changed	Where Changed	Object Type	What Changed	Video
	Removed	ENTERPRISE \Administrat or	5/6/2013 8:25:14 AM	10.0.0.15 1	Add or Remove Programs	Add or Remove Programs\Skype™ 5.3	B
	Installed	For: All users"					
	Version: 5	5.3.108"					
		Page 1 of 1	Le 1 for Char	etWri	X, ince "	www.netwrix.com	

Figure 68: Reports: All Changes With Video

8.2. Excluding/Including Data Types from/in Reports

You can fine-tune Netwrix Windows Server Change Reporter by specifying various data types that you want to exclude from the product Reports and Change Summaries. This can be done by editing .txt configuration files located in the product installation folder. The table below provides a list of the product configuration files and their descriptions. The instructions on the syntax can be found in the beginning of each file. One entry per line is accepted.

File Name	Description
omitdblist.txt	Contains a list of objects to be excluded from SSRS-based Reports.
omitreportist.txt:	Contains a list of objects to be excluded from Change Summary emails.
omitstorelist.txt	Contains a list of objects to be excluded from Change Summary emails.
omiterrors.txt	Contains a list of errors/warnings to be omitted from Change Summary emails or Session details.

Table 11: Netwrix Windows Server Change Reporter Configuration Files

A APPENDIX: MONITORED COMPONENTS AND SETTINGS

This section provides a full list of all components and settings monitored by Netwrix Windows Server Change Reporter. The **Who Changed** value is reported as "Not Applicable" for the components and settings marked with asterisk (*).

A.1 General Computer Settings

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

Table 12.	Monitored (Ohiects	Computer	Settinas
Tuble 12.	Montoreu	objects.	computer	Sectings

A.2 Add/Remove Programs

Table 13: Mon	nitored Objects:	Software	Installation
---------------	------------------	----------	--------------

Object Type	Attributes
Add or Remove Programs	Installed For*
	Version

A.3 Services

	A 11 .
Object Type	Attributes
System Service	Action in case of failed service startup
	Allow service to interact with desktop
	Caption
	Description
	• Name
	Path to executable
	Service Account
	Service Type
	Start Mode

Table 14: Monitored Objects: Services

A.4 Hardware

Object Type	Attributes
Base Board*	Hosting Board
	• Status
	Manufacturer
	Product
	Version
	Serial Number
BIOS*	Manufacturer
	Version
Bus*	Bus Type
	• Status
Cache Memory*	Configuration Manager Error Code
	Last Error Description
	Last Error Code
	Purpose
	• Status
CD-ROM Drive*	Configuration Manager Error Code
	Last Error Description
	Last Error Code
	Media Type
	Name
	SCSI Bus
	SCSI Logical Unit
	SCSI Port
	SCSI Target ID
	• Status
Disk Partition*	Primary Partition
	• Size (bytes)
	Starting offset (bytes)
Display Adapter*	Adapter RAM (bytes)

	Adapter Type
	Bits/Pixel
	Configuration Manager Error Code
	Driver Version
	Installed Drivers
	Last Error Description
	Last Error Code
	Refresh Rate
	Resolution
	Status
DMA*	
	• Status
Floppy Drive"	Configuration Manager Error Code
	Last Error Description
	Last Error Code
	• Status
Hard Drive*	Bytes/Sector
	Configuration Manager Error Code
	Interface Type
	Last Error Description
	Last Error Code
	Media Loaded
	• Media Type
	• Model
	Partitions
	SCSI Bus
	SCSI Logical Unit
	SCSI Port
	SCSI Target ID
	Sectors/Track
	• Size (bytes)
	• Status
	Total Cylinders
	Total Heads
	Total Sectors
	Total Tracks
	Tracks/Cylinder
IDE*	Configuration Manager Error Code
	Description
	Last Error Description
	Last Error Code
	• Status
Infrarad*	- Configuration Manager Error Code
	Last Error Code
	• Status
Keyboard*	Configuration Manager Error Code
	Description
	Last Error Description
	Last Error Code

	• Name
	Status
Logical Disk*	Description
	File System
	• Size (bytes)
	• Status
A4*	Confirmation Honoron France Code
Monitor	Configuration manager Error Code
	Last Error Description
	Last Error Code
	Monitor Type
	• Status
Network Adapter	Adapter Type
	Configuration Manager Error Code
	Default IP Gateway
	DHCP Enabled
	DNC Server Search Order
	• DNS Server search order
	• IP Address
	Last Error Description
	Last Error Code
	MAC Address
	Network Connection Name
	Network Connection Status
	Service Name
	• Status
Network Protocol*	Description
	Status
Parallal Ports*	 Configuration Manager Error Code
	Colliguation Manager Error Code
	Last Error Description
	Last Error Code
	Status
PCMCIA Controller*	Configuration Manager Error Code
	Last Error Description
	Last Error Code
	• Status
Physical Memory*	Capacity (bytes)
Thysical memory	• Status
	• Manuacturer
	• memory Type
	• Speed
	Part Number
	Serial Number
Pointing Device*	Configuration Manager Error Code
	Double Click Threshold
	Handedness
	Hardware Type
	Last Error Description
	Last Error Code

	Number of buttons
	• Status
Printing	Comment*
-	Hidden*
	• Local*
	Location*
	Name*
	Network*
	Port Name*
	Printer error information
	Published*
	Shared*
	Share Name*
	• Status
Processor*	Configuration Manager Error Code
	Last Error Description
	Last Error Code
	Max Clock Speed (MegaHertz)
	Name
	• Status
SCSI*	Configuration Manager Error Code
	Description
	Last Error Description
	Last Error Code
	• Status
Serial Ports*	Configuration Manager Error Code
	Last Error Description
	Last Error Code
	Maximum Bits/Second
	Name
	• Status
Sound Device*	Configuration Manager Error Code
	Last Error Description
	Last Error Code
	• Status
System Driver	Description
	Error Control
	Start Mode
	Service Type
System Slot*	Slot Designation
-	Status
USB Controller*	Configuration Manager Error Code
	Last Error Description
	Last Error Code
	Name
	Status
USB Hub*	Configuration Manager Error Code
	Last Error Description

•	Last Error Code
•	Name
•	Status

A.5 Scheduled Tasks

Table 16	· Mo	nitored	Objects.	Scheduled	Tasks
Tuble To	<i>. พ</i> เบ	nitoreu	Objects.	Scheuuleu	TUSKS

Object Type	Attributes
Scheduled Task	Account NameApplication
	 Comment Creator Enabled
	ParametersTriggers

A.6 Local Users and Groups

Table 17: Monitored Objects: Local Users and Groups

Object Type	Attributes
Local Group	Description
	• Name
	Members
Local User	Description
	Disabled/Enabled
	• Full Name
	• Name
	User cannot change password
	Password Never Expires
	User must change password at next logon

A.7 DNS Configuration*

Object Type	Attributes
DNS Server	Address Answer Limit
	Allow Update
	Auto Cache Update
	Auto Config File Zones
	Bind Secondaries
	Boot Method
	Default Aging State
	Default No Refresh Interval
	Default Refresh Interval
	Disable Auto Reverse Zones

Table 18: Monitored Objects: DNS Configuration
	Disjoint Nets	
	Ds Available	
	Ds Polling Interval	
	Ds Tombstone Interval	
	EDns Cache Timeout	
	Enable Directory Partitions	
	Enable Dns Sec	
	Enable EDns Probes	
	Event Log Level	
	Forward Delegations	
	Forwarders	
	Forwarding Timeout	
	Is Slave	
	Listen Addresses	
	Local Net Priority	
	Log File Max Size	
	Log File Path	
	Log IP Filter List	
	Log Level	
	Loose Wildcarding	
	Max Cache TTL	
	Max Negative Cache TTL	
	Name Check Flag	
	No Recursion	
	Recursion Retry	
	Recursion Timeout	
	Round Robin	
	Rpc Protocol	
	Scavenging Interval	
	Secure Responses	
	Send Port	
	Server Addresses	
	Strict File Parsing	
DNS Zone	• Aging State	
	Allow update	
	Auto created	
	Availability for scavenge time	
	Data file name	
	Ds integrated	
	Expires after	
	Forwarder slave	
	Forwarder timeout	
	Last successful soa check	
	Last successful Xfr	
	Master servers	
	Minimum TTL	
	No refresh interval	
	Notify	
	Notify servers	
	Owner name	

	Paused
	Primary server
	Refresh interval
	Refresh interval
	Responsible person
	Retry interval
	Reverse
	Scavenge servers
	Secondary servers
	Secure secondaries
	Shutdown
	• TTL
	Use wins
	Zone type
DNS Domain	Container Name

A.8 DNS Resource Records*

Table 19:	Monitored Objects: DNS Resource Records
-----------	-----------------------------------------

Object Type	Attributes
DNS AAAA	 Container name IPv6 Address Owner name TTL
DNS AFSDB	 Container name Owner name Server name Server subtype TTL
DNS ATM A	 ATM Address Container name Format Owner name TTL Value
DNS A	 Container name IP Address Owner name TTL
DNS CNAME	 Container name FQDN for target host Owner name TTL
DNS DHCID	 Container name DHCID (base 64) Owner name TTL

DNS DNAME	Container name
	FODN for target domain
	Owner name
	• TTL
	- Algorithm
	Algoritim Container name
	• Key type
	• Key (base 64)
	• Name type
	• Owner name
	Protocol
	• Signatory field
	• IIL
DNS DS	Key tag
DNS HINFO	Container name
	CPU type
	Operating system
	Owner name
	• TTL
DNS ISDN	Container name
	ISDN phone number and DDI
	ISDN subaddress
	Owner name
	• TTL
DNS KEY	Algorithm
	Container name
	Key type
	• Key (base 64)
	Name type
	Owner name
	Protocol
	Signatory field
	• TTL
DNS LOC	Container name
	MF host
	Owner name
	• TTL
DNS MB	Container name
	Mailbox host
	Owner name
	• TTL
DNS MD	Container name
	MD host
	Owner name
	• TTL
DNS MF	Container name
	MF host
	Owner name
	1

	• TTL
DNS MG	Container name
	Member mailbox
	Owner name
	TTI
DNS MINFO	Container name
	Error mailbox
	Owner hand Decoorcible mailbox
	 Responsible manbox TTI
DNS MK	Container name
	Owner name
	• Replacement mailbox
	• 11L
DNS MX	Container name
	FQDN of mail server
	Mail server priority
	Owner name
	• 11L
DNS NAPTR	Container name
	Flag string
	• Order
	Owner name
	Preference
	Regular expression string
	Replacement domain
	• Service string
	• 11L
DNS NS	Container name
	Name servers
	Owner name
	• 11L
DNS NXT	Container name
	Next domain name
	Owner name
	Record types
	• TTL
DNS PTR	Container name
	Owner name
	PTR domain name
	• TTL
DNS Resource Record	Owner name
	Record class
	• TTL
	Zone type
DNS RP	Container name
	Mailbox of responsible person
	• Optional associated text (TXT) record

	Owner name
	• TTL
DNS RRSIG	Algorithm
	Container name
	Key tag
	Labels
	Original TTL
	Owner name
	Signature expiration (GMT)
	Signature inception (GMT)
	• Signature (base 64)
	Signer's name
	• TTL
	Type covered
DNS RT	Container name
	Intermediate host
	Owner name
	Preference
	• TTL
DNS SIG	Algorithm
	Container name
	• Key tag
	• Labels
	Original TTL
	Owner name
	Signature expiration (GMT)
	• Signature inception (GMT)
	• Signature (base 64)
	Signer's name
	• TTL
	Type covered
DNS SRV	Container name
	Host offering this service
	Owner name
	Port number
	Priority
	• TTL
	Weight
DNS TEXT	Container name
	Owner name
	• Text
	• TTL
DNS WINS	Cache time-out
	Container name
	Do not replicate this record
	Lookup time-out
	Owner name
	Wins servers
DNS WINSR	Cache time-out

	Container name
	Domain to append to returned name
	Do not replicate this record
	Lookup time-out
	Owner name
	Submit DNS domain as NETBIOS scope
DNS WKS	Container name
	IP address
	Owner name
	Protocol
	Services
	• TTL
DNS X25	Container name
	Owner name
	Record
	• TTL
	X.121 PSDN address

A.9 Windows Registry Settings

Object Type	Attributes
OS Security	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\FileSystem(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\NetworkProvider(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\Print\\Providers\\LanMan Print Services(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SecurePipeServers(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SessionManager\\Environment(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SessionManager\\SubSystems(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SessionManager\\Memory Management(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SessionManager\\Executive(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SessionManager\\KnownDLLs(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\Windows(\\.*)
	 HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Image File ExecutionOptions(\\.*)
Security Settings	 HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\DrWatson(\\.*)
	 HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Driver Signing(\\.*)
	 HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Non-Driver Signing(\\.*)
	 HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE))

Table 20: Monitored Objects: Windows Registry Settings

	\\Microsoft\\MSDIC(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\NetDDE(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows\\CurrentVersion\\Policies\\System(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Explorer\\BitBucket(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Group Policy(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Installer(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE)) \\Microsoft\\Windows NT\\CurrentVersion\\Policies\\Explorer(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Policies\\System(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE)) \\Microsoft\\Windows NT\\CurrentVersion\\policies\\Network(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\policies\\Ratings(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\policies\\system(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\AEDebug(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\AsrCommands(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Perflib(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\SeCEdit(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Setup\\RecoveryConsole(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Winlogon(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE)) \\Policies\\Microsoft\\PCHealth\\ErrorReporting(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE)) \\Policies\\Microsoft\\Conferencing(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\EventViewer(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Messenger\\Client(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\SearchCompanion(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\SystemCertificates\\AuthRoot(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\W32time\\Parameters(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows NT\\DCOM(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows NT\\IIS(\\.*)
•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows NT\\Printers(\\.*)

	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows NT\\Rpc(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows\\DriverSearching(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows\\Group Policy(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows\\Installer(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows\\Internet Connection Wizard(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows\\Network Connections(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Windows\\Registration Wizard Control(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\Peernet(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\WindowsFirewall\\ StandardProfile\\IcmpSettings(\\.*)
	•	HKEY_LOCAL_MACHINE\\System\\Clone(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\Control\\SessionManager(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\WinLogon(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\CrashControl(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\FileSystem(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\LSA(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\Print\\Providers\\LanManPrint Services\\Servers(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\ProductOptions(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SecurePipeServers\\WinReg(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SessionManager\\kernel(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\WMI\\Security(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Enum(\\.*)
	•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Hardware Profiles(\\.*)
	•	HKEY_USERS\\.DEFAULT\\Software\\ Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer(\\.*)
	•	HKEY_USERS\\.Default\\Software\\Microsoft\\NetDDE(\\.*)
	•	HKEY_USERS\\.Default\\Software\\Microsoft\\ SystemCertificates\\Root\\ProtectedRoots(\\.*)
Patches	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Microsoft\\Windows NT\\CurrentVersion\\Hotfix(\\.*)
Windows Firewall	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\WindowsFirewall\\DomainProfile(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\WindowsFirewall\\StandardProfile(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\cryptography(\\.*)
	•	HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE) \\Policies\\Microsoft\\windows\\safer\\codeidentifiers(\\.*)

Remote Desktop	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\Terminal Server\\WinStations\\RDP-Tcp(\\.*)
	 HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE)\\ Policies\\Microsoft\\Windows NT\\Terminal Services(\\.*)
File Sharing Settings	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\LanmanServer\\Shares(\\.*)
USB devices	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\USBSTOR(\\.*)
Important Services	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Schedule(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WebClient(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WmiApSrv(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\upnphost(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AFD(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Alerter(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AppMgmt(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AppMgr(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Appmon(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\BINLSVC(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\ \Services\\Browser(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Cdrom(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\CiSvc(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Clipsrv(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\Eventlog\\Application(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\Eventlog\\Security(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\Eventlog\\System(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\Fax(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\HTTPFilter(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\IISADMIN(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\IPSEC(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\LanManServer\\Parameters(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\LanmanWorkstation\\Parameters(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\LicenseService(\\.*)
	 HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\

	Services\\MSDTC(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MSFtpsvc(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MacFile(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MacPrint(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Messenger(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MrxSmb(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NTDS(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\NWCWorkstation(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NetBT(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Netlogon(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Netman(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NntpSvc(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NtFrs(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\POP3Svc(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RDSessMgr(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RasAuto(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RasMan(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RemoteAccess(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RemoteRegistry(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\Remote_Storage_Server(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Services\\Remote_Storage_User_Link(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RpcLocator(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SMTPSVC(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SNMPTRAP(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SNMP(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SharedAccess(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Spooler(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SrvcSurg(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TapiSrv(\\.*)
•	HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\

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

B APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support Netwrix Windows Server Change Reporter:

Document Name	Overview
Netwrix Windows Server Change Reporter Administrator's Guide	The current document.
<u>Netwrix Windows Server Change Reporter</u> <u>Installation Guide</u>	Provides detailed instructions on how to install NetWrix Windows Server Change Reporter, and explains how to configure the target Windows server for auditing.
<u>Netwrix Windows Server Change Reporter</u> <u>Release Notes</u>	Contains a list of the known issues that customers may experience with NetWrix Windows Server Change Reporter 4.0, and suggests workarounds for these issues.
<u>Netwrix Windows Server Change Reporter</u> Quick Start Guide	Provides an overview of the product functionality and instructions on how to install, configure and start using the product. This guide can be used for evaluation purposes.
<u>Netwrix Windows Server Change Reporter</u> <u>User Guide</u>	Provides the information on different Netwrix Windows Server Change Reporter reporting capabilities, lists all available reports and explains how they can be viewed and interpreted.
Netwrix Windows Server Change Reporter Freeware Edition Quick-Start Guide	Provides instructions on how to install, configure and use Netwrix Windows Server Change Reporter Freeware Edition.
Installing Microsoft SQL Server and Configuring the Reporting Services	This technical article provides instructions on how to install Microsoft SQL Server 2005/2008 R2/2012 Express and configure the Reporting Services.
How to Subscribe to SSRS Reports	This technical article explains how to configure a subscription to SSRS reports using the Report Manager.

Table 21: Product Documentation