



NETWRIX WINDOWS SERVER CHANGE REPORTER

USER 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. INTRODUCTION	4
1.1. Overview	4
1.2. How This Guide is Organized	4
2. PRODUCT OVERVIEW	5
2.1. Key Benefits	5
3. CHANGE SUMMARY	6
4. REPORTS	7
4.1. Reports List	7
4.2. Receiving Reports by Email	8
4.3. Viewing Reports in a Web Browser	9
5. CHANGE MANAGEMENT	11
5.1. Reviewing Changes to Monitored Components.....	11
A APPENDIX: RELATED DOCUMENTATION.....	14

1. INTRODUCTION

1.1. Overview

This guide is intended for the end users of Netwrix Windows Server Change Reporter. It contains the information on the product reporting capabilities, lists all available report types and report output formats, and explains how these reports can be viewed and interpreted.

This guide can be used by auditors, company management, or anyone who wants to view audit reports on the monitored environment.

1.2. How This Guide is Organized

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

- Chapter [1 Introduction](#): the current chapter. It explains the purpose of this document, defines its audience and outlines its structure.
- Chapter [2 Product Overview](#) provides an overview of the Netwrix Windows Server Change Reporter functionality.
- Chapter [3 Change Summary](#) shows a Change Summary example and explains what information a Change Summary contains.
- Chapter [4 Reports](#) contains an overview of the Reports functionality, lists all reports available in Netwrix Windows Server Change Reporter, provides their descriptions, and explains how to view reports in a web browser or receive them by email.
- Chapter [5 Change Management](#) contains an overview of the Change Management functionality and explains how to review and set a status for a change made to server configuration.
- [Appendix: Related Documentation](#) contains a list of all documentation 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.

2.1. Key Benefits

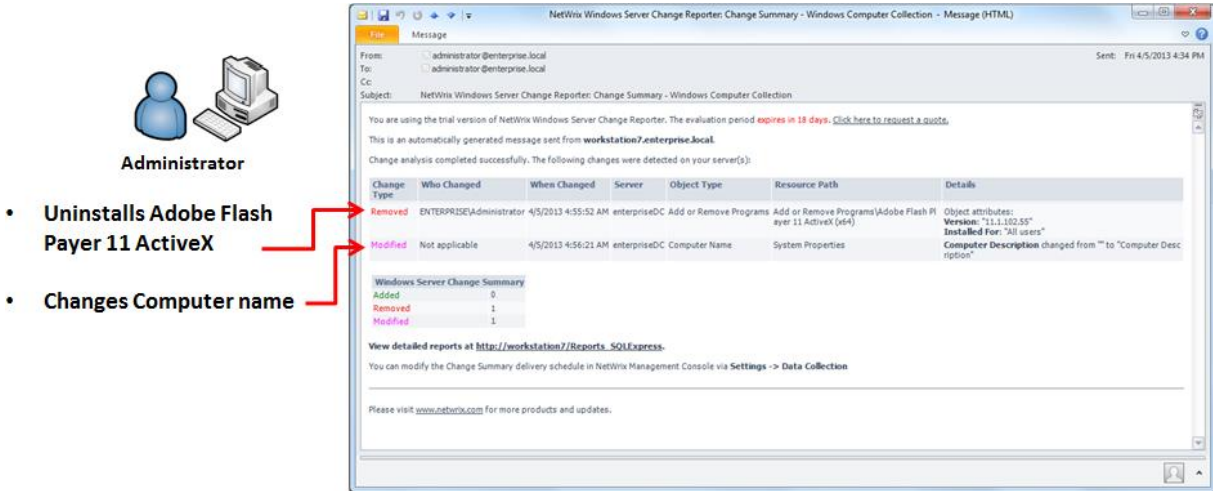
Netwrix Windows Server Change Reporter is a tool for automated auditing and reporting on changes made to the Windows server configuration. It allows you to do the following:

- **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:** the audit data on the Windows server configuration changes is stored in a central location, and the usage of the [AuditAssurance™ and AuditIntelligence™ technologies](#) 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.

3. 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:

Figure 1: Change Summary Example



The Change Summary provides the following information for each change:

Table 1: Change Summary Fields

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.

To receive daily Change Summary emails, ask your system administrator to add your email address to the Change Summary recipients list.

4. REPORTS

Netwrix Windows Server Change Reporter allows generating reports based on Microsoft SQL Server Reporting Services (SSRS). The product provides a wide variety of predefined report templates 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.

You can ask your system administrator to configure a subscription to the selected report (the list of available reports can be found in section [4.1 Reports List](#) of the current document), or you can view them through a web browser. For details on these options, refer to the following sections:

- [4.2 Receiving Reports by Email](#)
- [4.3 Viewing Reports in a Web Browser](#)

Note: If Netwrix Windows Server Change Reporter is configured to monitor multiple Managed Objects (collections of Windows servers), and to store collected audit data in several databases, viewing reports through a web browser will require your system administrator to perform some complex configuration steps. Ensure that your system administrator has performed the required configuration before viewing the report through a web browser.

4.1. Reports List

Netwrix Windows Server Change Reporter provides a variety of predefined report templates. If none of these reports suits your needs, you can [order a new custom report from Netwrix](#).

The table below lists all available reports and provides their descriptions:

Table 2: Reports List

Report Name	Description
Overview	
Overview (Chart)	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.
Change Management	
Change Review History	Shows all changes made to Windows server configuration. This report is an auxiliary tool that can be used in the change management process. For more details refer to chapter 5 Change Management of the current document.
Hardware and Software	
Add or Remove Programs	Shows added or removed programs, including the information on their versions and assignment to specific users or groups.
Hardware Changes	Shows all changes made to hardware components, such as hard drive, keyboard, network adapter, and so on.
Printer Changes	Shows changes made to printer settings, for example, error description, location, status, and so on.
Network Services reports	
DNS Configuration changes	Shows general DNS configuration changes, for example, zone, properties, and so on.
DNS Resource Record Changes	Shows changes, assignments and modifications made to all DNS resource record types.

Overall Changes reports	
All Server Changes by Date (Chart)	A chart report showing an overview of the changes to server configuration grouped by date. The data can be filtered by a date range and a monitored system component.
All Server Changes by Date	Shows all changes made to server configuration grouped by date.
All Server Changes by Object Type	Shows all changes made to server configuration grouped by a monitored component.
All Server Changes by User (Chart)	A chart report showing an overview of the changes made to server configuration grouped by the users who made the changes.
All Server Changes by User	Shows all server changes made to server configuration grouped by the users who made the changes.
All Server Changes	Shows all change made to all monitored components. The data can be filtered by date, server name and the monitored component.
System and Security reports	
General Computer Settings Changes	Shows changes made to system properties, for example, Computer name, General settings, Startup and Recovery information, and so on.
Local Users and Groups Changes	Shows changes made to local users and groups, for example, to such settings as local group name, members, local user description and so on.
Scheduled Tasks Changes	Shows changes made to scheduled tasks settings, such as account name, triggers, application and so on.
Services Changes	Shows changes made to services, for example changes to service account, service type and others.
Windows Registry Changes	Shows changes made to Windows Registry, such as the before and after values of a registry key, changes to permissions and so on.

Every report has a set of filters helping to manage the collected audit data in the most convenient way. It may vary depending on the selected report. The filters can be the following: time frame, date, object type, WHAT changed, WHO changed, WHERE changed, and so on.

4.2. Receiving Reports by Email

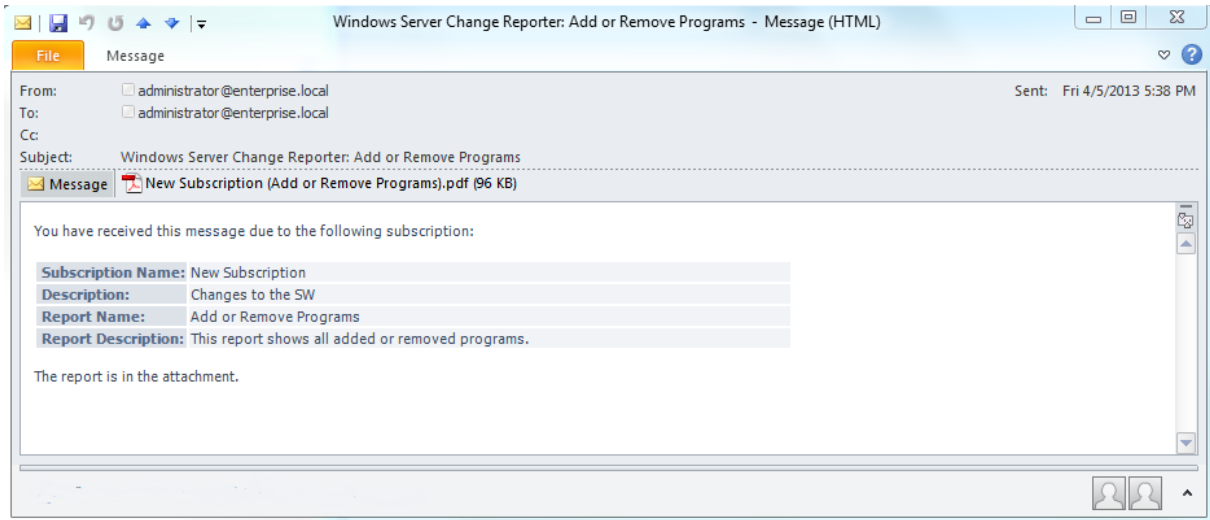
If you want to receive reports by email, ask your system administrator to configure a subscription to the selected reports. The administrator can configure report filters, so that you only receive the information you need, and select report output format: Excel, Word or PDF.

Reports can be delivered on one of the following schedules:

- On a daily basis (reports will be delivered every day at 3:00 AM);
- On a weekly basis (reports will be delivered on the specified days of the week at 3:00 AM);
- On a monthly basis (reports will be delivered in the specified months on a selected date at 3:00 AM).

Reports will be delivered as email attachments in the selected format:

Figure 2: Report Delivered by Subscription



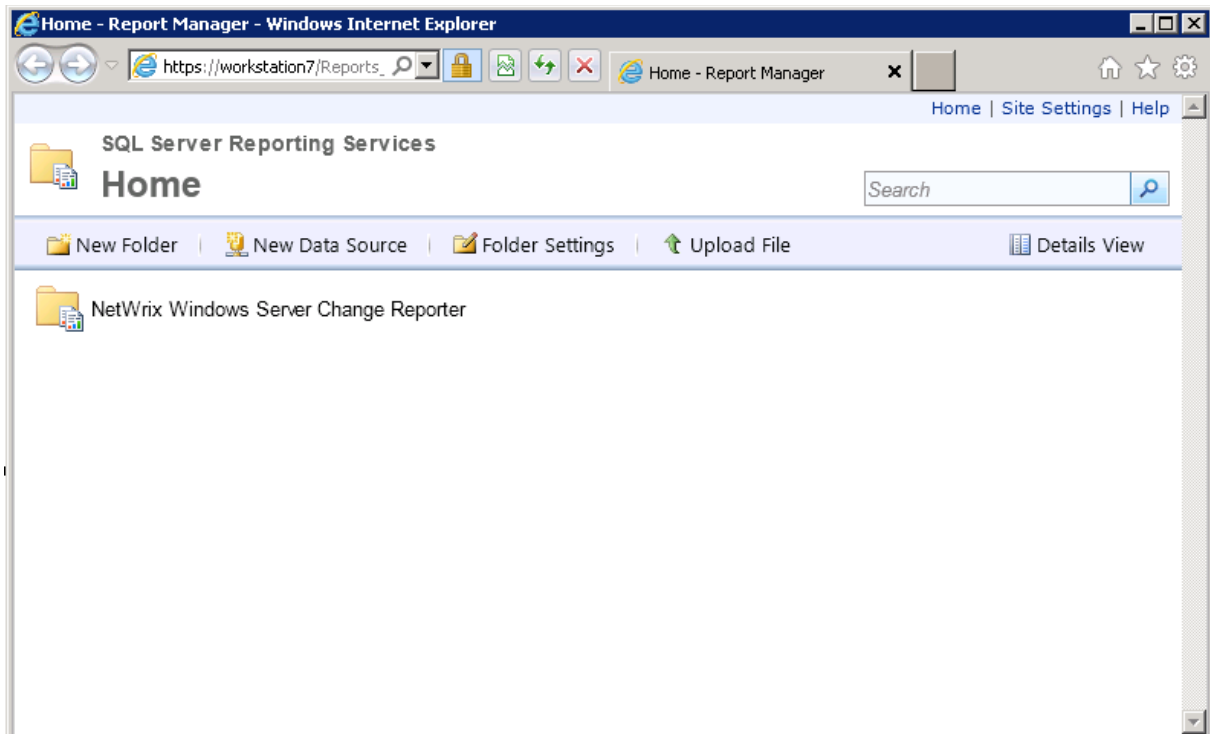
4.3. Viewing Reports in a Web Browser

To be able to view reports in your web browser, ask your system administrator to provide you with the Report Manager URL.

Procedure 1. To view reports in a web browser

1. In your web browser, type the Report Manager URL in the address line and press **Enter**. The SQL Server Reporting Services Home page will open:

Figure 3: Report Manager Home Page



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 the report page, you can specify filters to the selected report (report filters may vary depending on the selected report) and click the **View Report** button (**View Chart** for chart reports) to apply them:

Figure 4: All Windows Server Changes Report (Web Browser)

The screenshot shows the 'All Server Changes' report page. At the top, there are filter controls for 'Time frame', 'From', 'To', 'Sort By', 'What Changed', 'Who Changed', 'Where Changed', and 'Managed Object'. Below these is a table of 'Applied filters' showing the current values. The main content is a table of server changes with columns for Action, Who Changed, When Changed, Where Changed, Object Type, and What Changed. The table lists several changes related to scheduled tasks and user accounts.

Available filters →

Applied filters →

Changes made to the server →

Filter	Value
From:	2/26/2013 8:19:37 AM
To:	2/27/2013 8:19:37 AM
Sort By:	When Changed
What Changed:	%
Who Changed:	%
Where Changed:	%
Object Type:	%
Managed Object:	%

Action	Who Changed	When Changed	Where Changed	Object Type	What Changed
Modified	ENTERPRISE\WORKSTATIONS	2/26/2013 10:27:15 AM	workstation	Scheduled Task	Scheduled Task of Microsoft Windows\Customer Experience Improvement Program\Server\ServerFeedbackCollector
Triggers: Added: "At 2/26/2013 1:26:50 AM on 2/28/2013 1:26:50 AM - After triggered, repeat every 12:00:00 indefinitely"; Removed: "At 2/26/2013 7:17:14 AM on 2/26/2013 7:17:14 AM - After triggered, repeat every 12:00:00 indefinitely";					
Modified	ENTERPRISE\WORKSTATIONS	2/26/2013 10:27:15 AM	workstation	Scheduled Task	Scheduled Task of Microsoft Windows\Customer Experience Improvement Program\Server\ServerFeedbackCollector
Triggers: Added: "At 2/26/2013 1:26:50 AM on 2/28/2013 1:26:50 AM - After triggered, repeat every 12:00:00 indefinitely"; Removed: "At 2/26/2013 7:17:14 AM on 2/26/2013 7:17:14 AM - After triggered, repeat every 12:00:00 indefinitely";					
Added	ENTERPRISE\Administrator	2/27/2013 1:14:20 AM	workstation	Scheduled Task	Scheduled Task of Netwrix Management Console - Windows Server Change Reporter - c:\msc
Account Name: "ENTERPRISE\Administrator"					
Application: "C:\Program Files (x86)\Netwrix\Windows Server Change Reporter\SCCR.exe"					
Comment: ""					
Creator: "administrator"					

Note: Every chart report has a drill-down functionality. When viewing such report you can navigate to the next level of details by clicking one of the segments in a chart.

5. 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. Netrix 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 Netrix 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*.

5.1. Reviewing Changes to Monitored Components

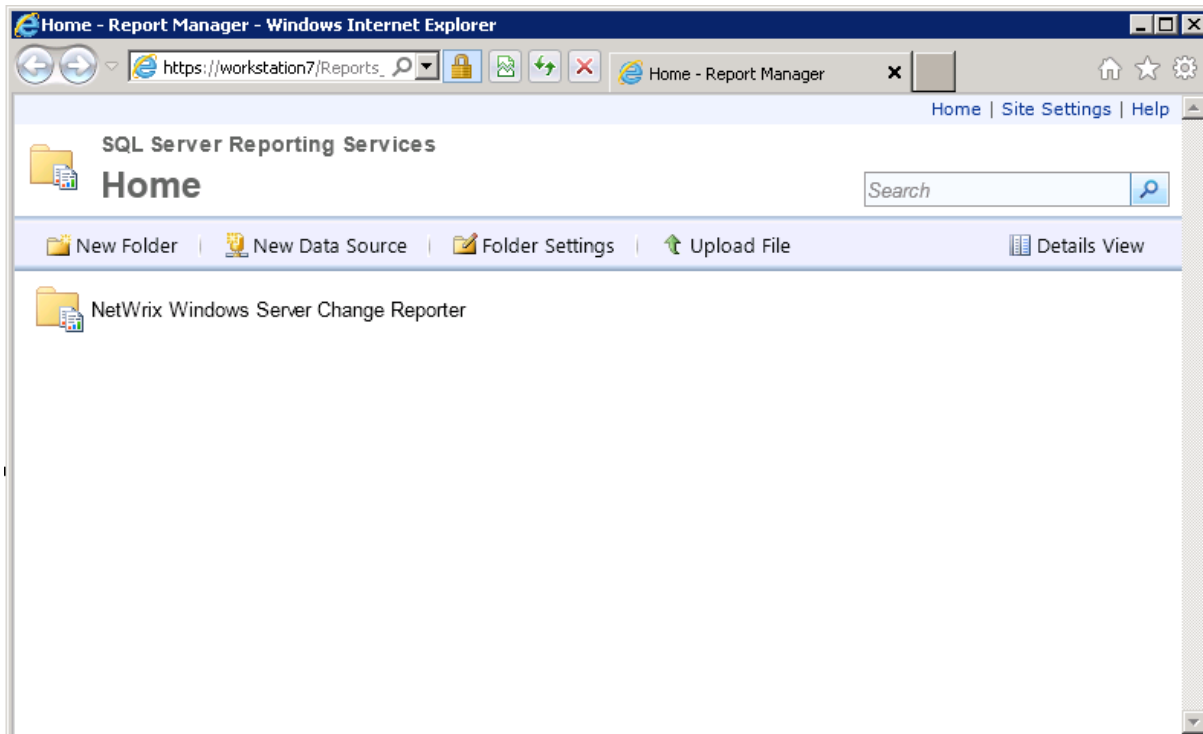
To be able to review changes and assign their statuses you need to open the *Change Review History* report in a web browser.

Note: Ensure that your system administrator has performed the required configuration before starting to manage reports in a web browser.

Procedure 2. To review changes made to Windows server configuration

1. In your web browser, type the Report Manager URL in the address line and press **Enter**. The SQL Server Reporting Services Home page will open:

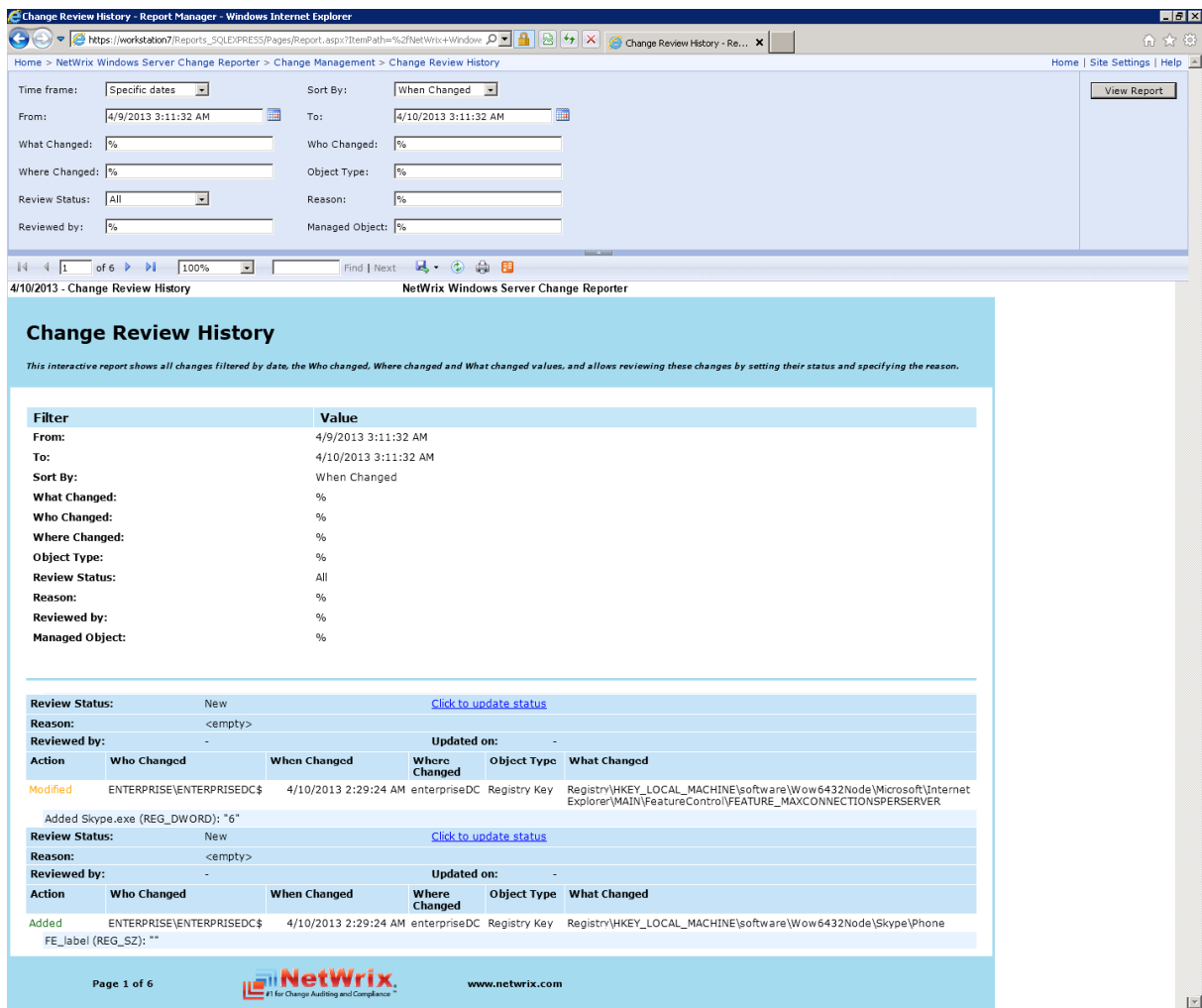
Figure 5: Report Manager Home Page



2. Click the **Netrix Windows Server Change Reporter** folder and navigate to the *Change Review History* report.

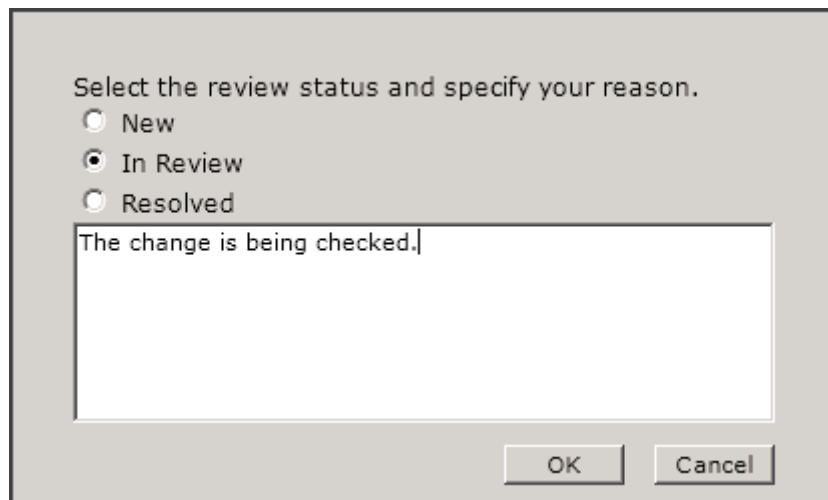
- Specify filters to the report and click the **View Report** button to apply them. The report will be displayed showing the changes made to Windows server configuration within the specified time frame:

Figure 6: Change Review History Report



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

Figure 7: Status update window (Web Browser)



Note: 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.

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

Figure 8: Updated status (Web Browser)

Review Status:	In Review		Click to update status		
Reason:	Change is being checked.				
Reviewed by:	ENTERPRISE\administrator		Updated on:	4/10/2013 6:45:21 AM	
Action	Who Changed	When Changed	Where Changed	Object Type	What Changed
Added	ENTERPRISE\Administrator	4/10/2013 2:29:30 AM	enterpriseDC	Add or Remove Programs	Add or Remove Programs\Skype™ 5.3
Installed For: "All users"					
Version: "5.3.108"					

A APPENDIX: RELATED DOCUMENTATION

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

Table 3: Product Documentation

Document Name	Overview
Netwrix Windows Server Change Reporter User Guide	The current document
Netwrix Windows Server Change Reporter Administrator's Guide	Provides a detailed explanation of the Netwrix Windows Server Change Reporter features and step-by-step instructions on how to configure and use the product.
Netwrix Windows Server Change Reporter Installation and Configuration Guide	Provides detailed instructions on how to install NetWrix Windows Server Change Reporter, and explains how to configure the target Windows server for auditing.
Netwrix Windows Server Change Reporter Release Notes	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.
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.
Netwrix Windows Server Change Reporter 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.
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.