# NETWRIX WINDOWS SERVER CHANGE REPORTER

## FREEWARE EDITION

## QUICK-START 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.

# Table of Contents

# 1. INTRODUCTION

## 1.1. Overview

This guide is intended for the first-time users of Netwrix Windows Server Change Reporter Freeware Edition. It contains the information on the product functionality and provides instructions on how to install, configure and use the product.

The guide can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided.

> **Note:** The guide only covers simple installation and configuration options applicable to Netwrix Windows Server Change Reporter Freeware Edition. The information on the Enterprise Edition of the product can be found in the documentation provided in section A Appendix: Related Documentation.

## 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 Installing Netwrix Windows Server Change Reporter Freeware provides instructions on how to install Netwrix Windows Server Change Reporter Freeware Edition.

- Chapter 4 Configuring Netwrix Windows Server Change Reporter Freeware provides detailed instructions on how to configure Netwrix Windows Server change Reporter Freeware Edition.

- Chapter 5 Viewing Changes to Server Configuration shows an example of Change Summary and explains how to generate it on demand, view it via Report Viewer and change its delivery schedule.

- 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 and Features

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.

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 details of 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 configuration changes data at any time. The retention period can be changed according to your needs.

**Note:** Not all the features listed above are available in Netwrix Windows Server Change Reporter Freeware Edition. For the details on the difference between Freeware and Enterprise Editions, refer to section 2.2 Product Editions.

## 2.2. 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.

Table 1: below outlines the differences between the Netwrix Windows Server Change Reporter Editions:

*Table 1:    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<br>Create manually or order from Netwrix |
| 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<br>Data is only stored for 2 days | Yes<br>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 | Support Forum<br>Knowledge Base | Full range of options:<br>Phone, email, submission of support tickets, Support Forum, Knowledge Base |
| Licensing | Free of charge | Per server<br>Request a quote |

## 2.3. Netwrix Windows Server Change Reporter Freeware Edition Workflow

The Netwrix Windows Server Change Reporter Freeware Edition data collection and reporting workflow is the following:

*Figure 1:     The Netwrix Windows Server Change Reporter Freeware Edition workflow*
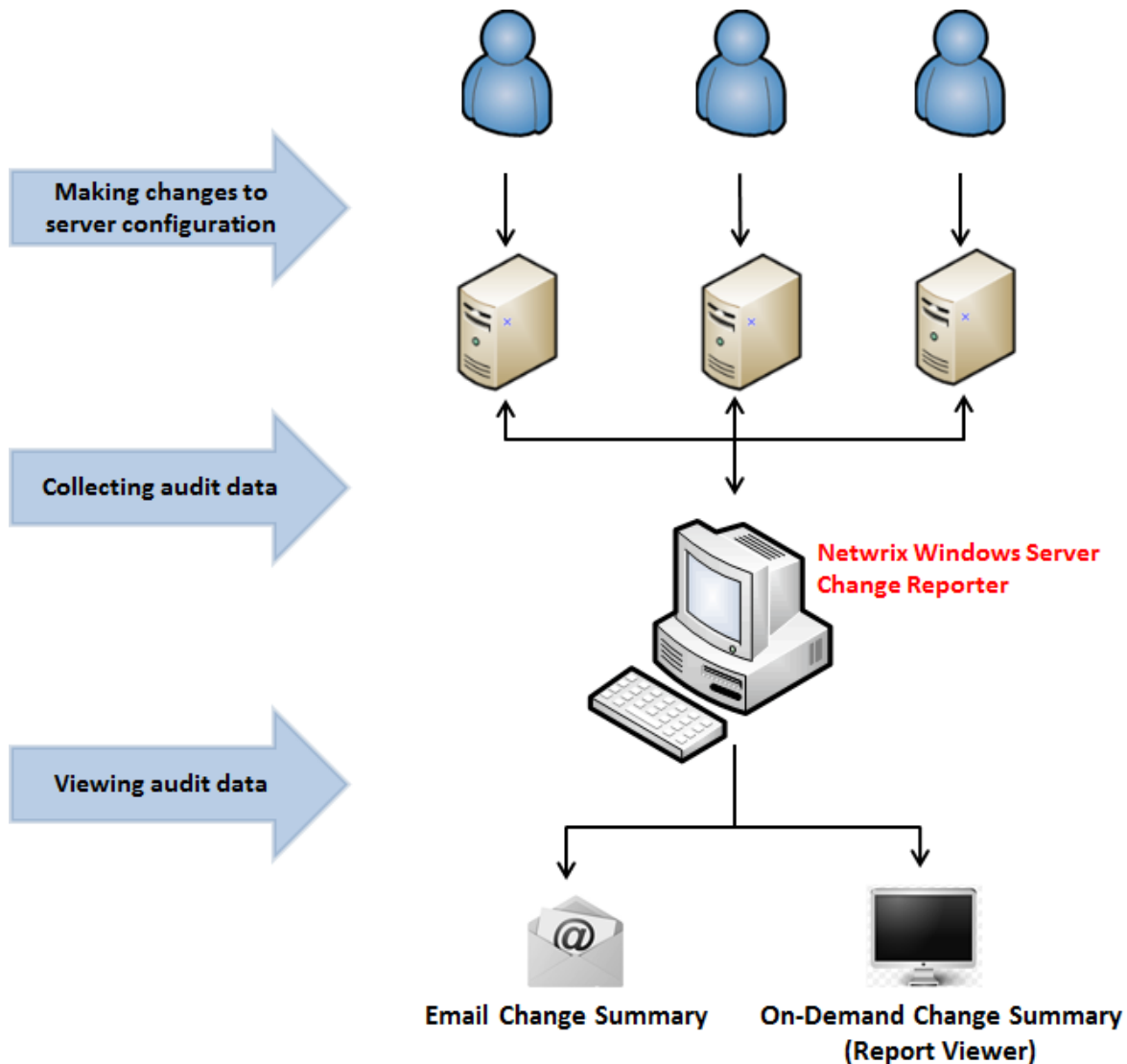


1. A system administrator configures Netwrix Windows Server Change Reporter by specifying the Windows servers and their components to be monitored for configuration changes.

2. A dedicated scheduled task which is launched daily collects the audit data and writes it to a local file-based storage referred to as Audit Archive. The task trigger parameters can be changed as required, or the task can be launched manually via Task Scheduler. Each data collection is referred to as a session.

3. After the task has been executed, a Change Summary containing a list of changes that occurred since the last data collection is sent to the specified recipients.

4. At the same time, server configuration changes become available for viewing via Report Viewer that allows generating On-Demand Change Summary for the specified time frame.

# 3. INSTALLING NETWRIX WINDOWS SERVER CHANGE REPORTER FREEWARE EDITION

## 3.1. Installation Prerequisites

This section provides hardware and software requirements necessary to use Netwrix Windows Server Change Reporter Freeware Edition, and recommendations on how to deploy this product.

### 3.1.1. Deployment Options

Netwrix Windows Server Change Reporter Freeware Edition can be installed on any computer of the domain containing the monitored servers. If the monitored servers belong to a different domain, a trust relationship between this domain and the domain where the product is installed should be established.

> **Note:** Netwrix Windows Server Change Reporter Freeware Edition requires remote access to a set of standard Windows services, such as Remote Registry, Windows Management Instrumentation (WMI), and so on. If your target servers are behind the Firewall, for configuration details refer to the following Netwrix Knowledge Base articles: How to audit servers located in another subnet behind firewall and Ports required to monitor servers over the firewall.

### 3.1.2. Hardware Requirements

Before installing Netwrix Windows Server Change Reporter Freeware Edition, make sure that your hardware meets the following requirements:

*Table 2:   Netwrix Windows Server Change Reporter Hardware Requirements*

| Hardware Component | Minimum | Recommended |
|---|---|---|
| Processor | Intel or AMD 32 bit, 500MHz | Intel or AMD 64 bit, 3GHz<br>Note: The Itanium (IA64) processor is not supported. |
| Memory | 512MB RAM | 2GB RAM |
| Disk space | 50MB | 20GB |

### 3.1.3. Software Requirements

Before installing Netwrix Windows Server Change Reporter Freeware Edition, make sure that your system meets the following software requirements:

*Table 3:   Netwrix Windows Server Change Reporter Software Requirements*

| Component | Requirement |
|---|---|
| Operating System | Windows XP SP3 or above |
| Framework | .NET Framework 3.5 |
| Additional Software | Windows Installer 3.1 or above |

### 3.1.4. Target Server Requirements

The following requirements apply to the monitored servers:

*Table 4:    Target Server Requirements*

| Component | Requirement |
|---|---|
| Operating System | Windows XP or above |
| Framework | .NET Framework 2.0, 3.0 or 3.5<br>NOTE: Only required if you enable the Network Traffic Compression product option. |
| Services | Make sure that the Remote Registry and Windows Management Instrumentation (WMI) services are started. |

## 3.2. Installing Netwrix Windows Server Change Reporter Freeware Edition

To install Windows Server Change Reporter Freeware Edition perform the following procedure:

**Procedure 1.   To install Netwrix Windows Server Change Reporter**

1.   Download Netwrix Windows Server Change Reporter.

2.   Run the setup package called **wscrfree_setup.msi**.

3.   Follow the instructions of the installation wizard.

4.   When prompted, accept the license agreement and specify the installation folder.

5.   On the last step, click **Finish** to accept the installation.

When the installation process is completed the product and the Report Viewer shortcuts will be added to the Start menu. If on the last step of the installation process the option to start the product is enabled, the product configuration dialog will be opened.
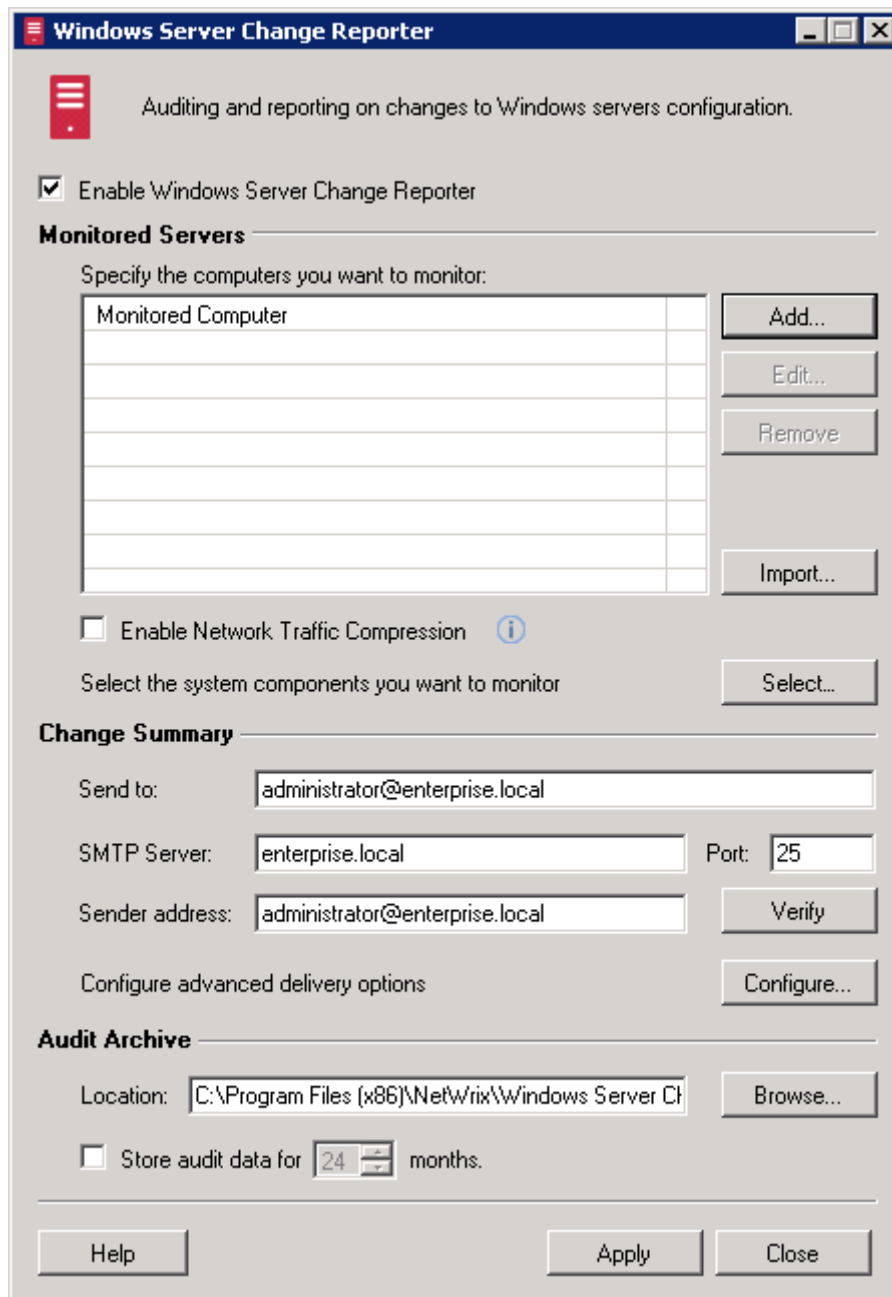
# 4. CONFIGURING NETWRIX WINDOWS SERVER CHANGE REPORTER FREEWARE EDITION

After Netwrix Windows Server Change Reporter has been successfully installed, it requires a certain manual configuration to be done.

**Procedure 2.   To Configure Netwrix Windows Server Change Reporter**

1. Navigate to **Start** → **All Programs** → **Netwrix Freeware** → **Windows Server Change Reporter** and click the **Windows Server Change Reporter** shortcut. The product configuration dialog will open:

*Figure 2:    The Netwrix Windows Server Change Reporter Configuration Dialog*



2. Specify the following settings and parameters:

> **Note:**   The table below describes configuration of the basic parameters required for the product evaluation purposes.

*Table 5:  Netwrix Windows Server Change Reporter Freeware Edition Settings*

| Parameter | Instruction |
|---|---|
| Enable Windows Server Change Reporter | Enable this option in order to activate Windows Server Change Reporter to collect information on server configuration changes. |
| Specify the monitored servers settings | |
| Servers | Enter the servers that you wish to monitor for configuration changes. You can use the FQDN or NETBIOS formats, or provide an IP address. |
| Enable Network Traffic Compression | Enable this option if you are using distributed multi-sites networks or the connection used for data transfer is slow. |
| Select the system components you want to monitor | Click the **Select** button to select the system components that you wish to monitor for changes. Note: By default, the components enabled in the *Monitored System Components* dialog are available for monitoring by Netwrix Windows Server Change Reporter Freeware Edition. To monitor other components, Enterprise Edition of the product is required. |
| Specify Change Summary delivery settings | |
| Send to: | Enter the email address of the Change Summary recipient; you can enter several addresses separated by a semicolon. |
| SMTP server: | Enter the SMTP server name. |
| Port: | Specify the SMTP port number (the default value is 25). |
| Sender address: | Enter the email address of the Change Summary sender. |
| Verify | Click to test the email settings of the recipient(s) you specified above. A test email will be sent to the recipients, or the product will inform in case of any problems with the email delivery. |
| Configure advanced delivery options | Click the **Configure** button if you wish to change the delivery schedule of a Change Summary. Note: Other settings are available for editing in Netwrix Windows Server Change Reporter Enterprise Edition only. |
| Specify audit archive settings | |
| Location | Leave the default setting or specify another path to save the audit data. |

3. Save your configuration by clicking the **Apply** button. The **Scheduled Task Credentials** dialog will be displayed.

4. Specify the account under which the product scheduled task will collect the audit data.

5. Ensure that this account has the following privileges:

   a. Local administrator rights on the computer with the product installed and the monitored servers;

   b. 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;

    c. If the computer with the product installed and the monitored servers belong to a 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.

    d. The "Log on as a batch job" policy defined for the account (for instructions, refer to Procedure 3 To define the Log on as a batch job policy for an account).

6. Enter and confirm the account password and click **OK**. The **NEXT STEPS: CHECKLIST** dialog will open; follow its instructions to get the first report right after you have configured the product. Otherwise, you will receive it as scheduled by default at 3:00 AM.

7. The product functions as a background process, and you do not need to keep it open once it has been configured. To change the settings later, invoke the product configuration dialog from the **Start** menu.

## Procedure 3. To define the Log on as a batch job policy for an account

1. On a domain controller, navigate to **Start → Administrative Tools → Group Policy Management**.

2. Expand the **Forest → Domains → <your_Domain> node**, right-click **Default Domain Policy** and select **Edit** from the popup menu.

3. In the **Group Policy Management Editor**, in the left pane, navigate to **Computer Configuration → Policies → Windows Settings Security Settings → Local Policies → User Rights Assignment** and locate the "Log on as a batch job policy" on the right:

*Figure 3:     Group Policy Management Editor*
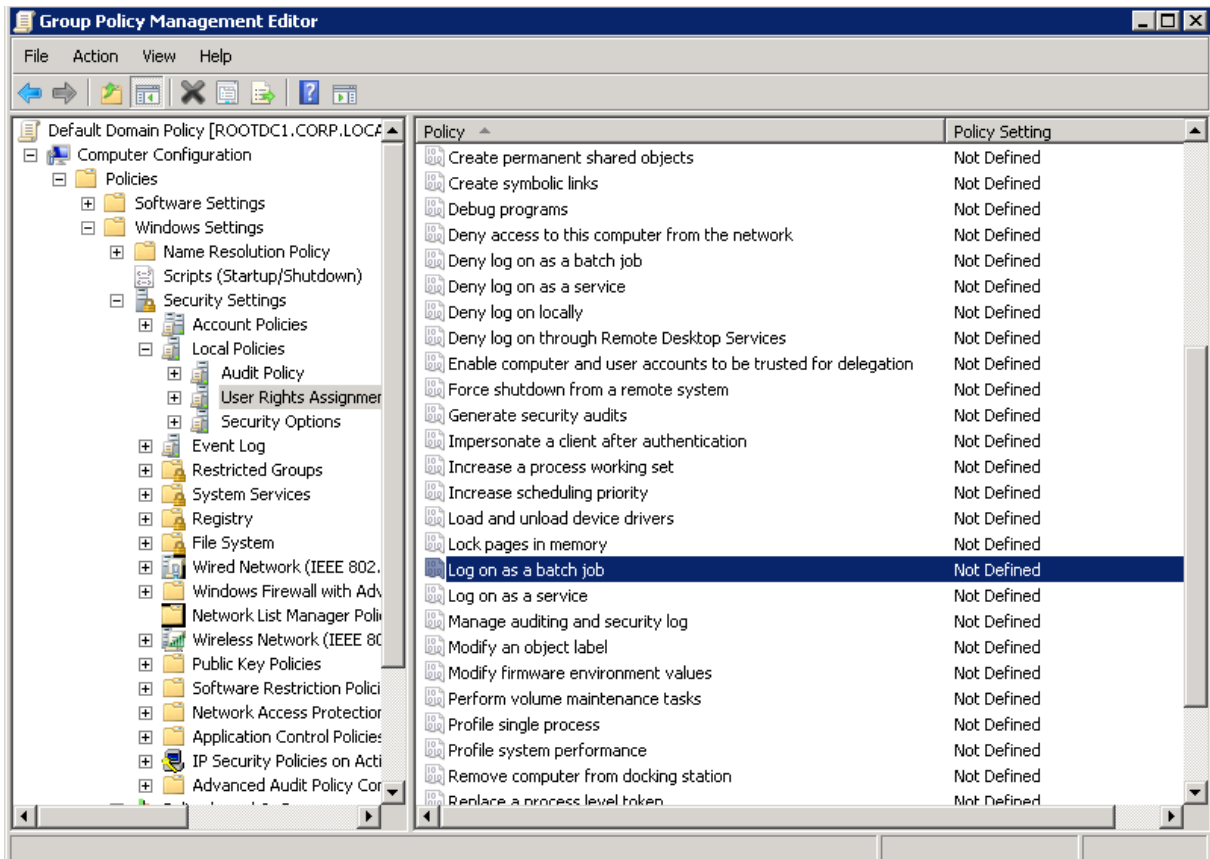
4. Double-click this policy. In the dialog that opens, select the **Define these policy settings:** option and click the **Add User or Group** button:

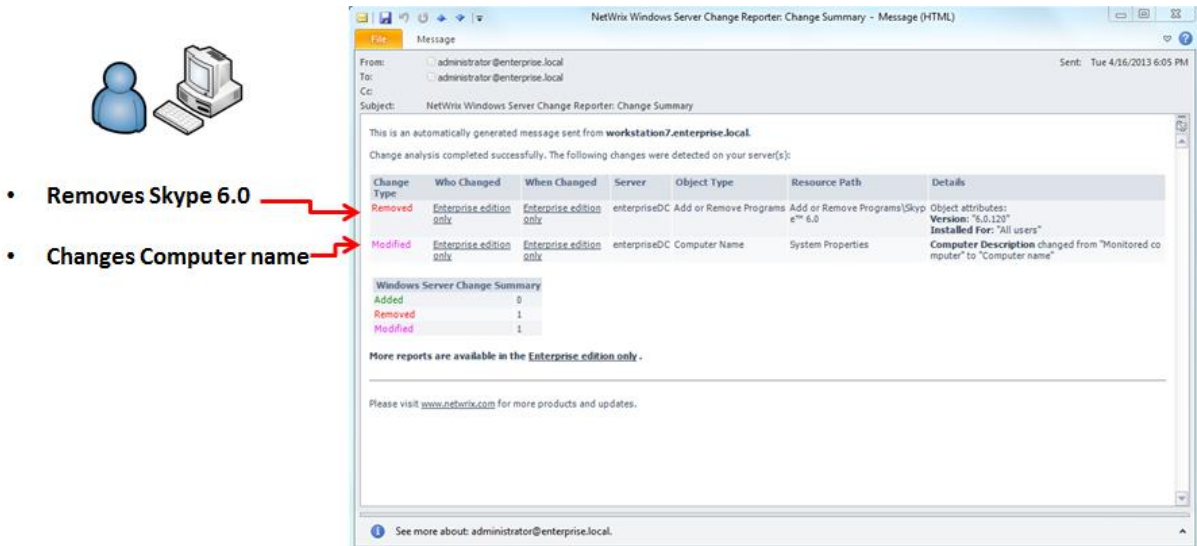*Figure 4:    Logon as a batch job Properties*
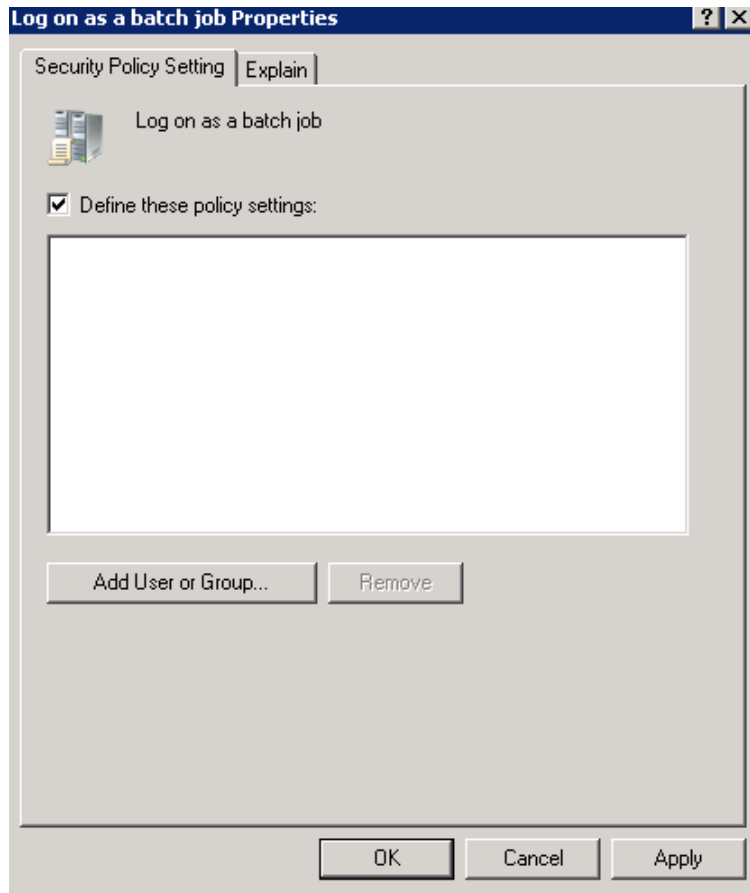


5. Specify the account that you want to define this policy for, and click **OK** to save the changes.

# 5. VIEWING CHANGES TO SERVER CONFIGURATION

During the Netwrix Windows Server Change Reporter installation, the task to collect server changes data is created. By default, it is scheduled to run automatically every day at 3:00 AM.

After the execution of the scheduled task has been completed, a Change Summary containing a list of all changes that occurred since the last data collection is generated and delivered to the specified recipients by email.

*Figure 5:     Change Summary Example*



The Change Summary provides the following information for each change:

- Change type, for example Added, Removed, Modified;

- Object Type, for example, Computer Name;

- WHERE the change occurred;

- Additional details on the change made to server configuration including the before and after values of the changed setting.

**Note:**    The Change Summary provided by Netwrix Windows Server Change Reporter Freeware Edition does not contain all the details that are provided by the Enterprise version of the product. For more details refer to Netwrix Windows Server Change Reporter Administrator's Guide.

If required, you can modify Change Summary delivery schedule and generate Change Summary on-demand

## 5.1. Modifying Change Summary Delivery Schedule

If you wish to change the default settings for the Change Summary delivery schedule, do the following:

**Procedure 4.   To Modify Change Summary Delivery Schedule:**

1.  Navigate to **Start** → **All Programs** → **Administrative Tools** → **Task Scheduler**.

2.  In the left pane, expand the **Task Scheduler Library** node. In the right pane, select the task called *Netwrix Windows Server Change Reporter*.

3.  Right-click the task, select **Properties** → **Triggers** and click **Edit.** Alternatively, use the **Properties** option from the **Actions** menu.

4.  Specify the details of the Change Summary delivery schedule and click **OK**.

## 5.2. 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 5.   Generating Change Summary on Demand:**

1.  Launch Task Scheduler.

2.  In the left pane, expand the **Task Scheduler Library** node. In the right pane, select the task called *Netwrix Windows Server Change Reporter*.

3.  Right-click the task and select **Run**, or alternatively, use the **Run** option from the **Actions** menu.

4.  Once the task execution has been finished, the report with the changes will be sent via email to the specified recipient.

## 5.3. 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 6.   To View Change Summary for the Specified Time Frame:**

1.  Navigate to **Start** → **All Programs** → **Netwrix Freeware** → **Netwrix Windows Server Change Reporter** → **Advanced Tools** and click the **Report Viewer** shortcut.

2.  Select **Windows server** for which you would like to view the changes from the drop-down list.

3.  Specify the time frame by selecting the sessions in the **From session** and **To session** drop-down lists.

4.  Click the **Generate Summary** button.

5.  You will be asked to save the result as an HTML document, to do that specify the file name and click **Save**.

6.  The changes made to server configuration within the specified time frame will be displayed in a web browser.

*Figure 6:     Change Summary (Report Viewer)*

Suggestions or comments about this document? www.Netwrix.com/feedback
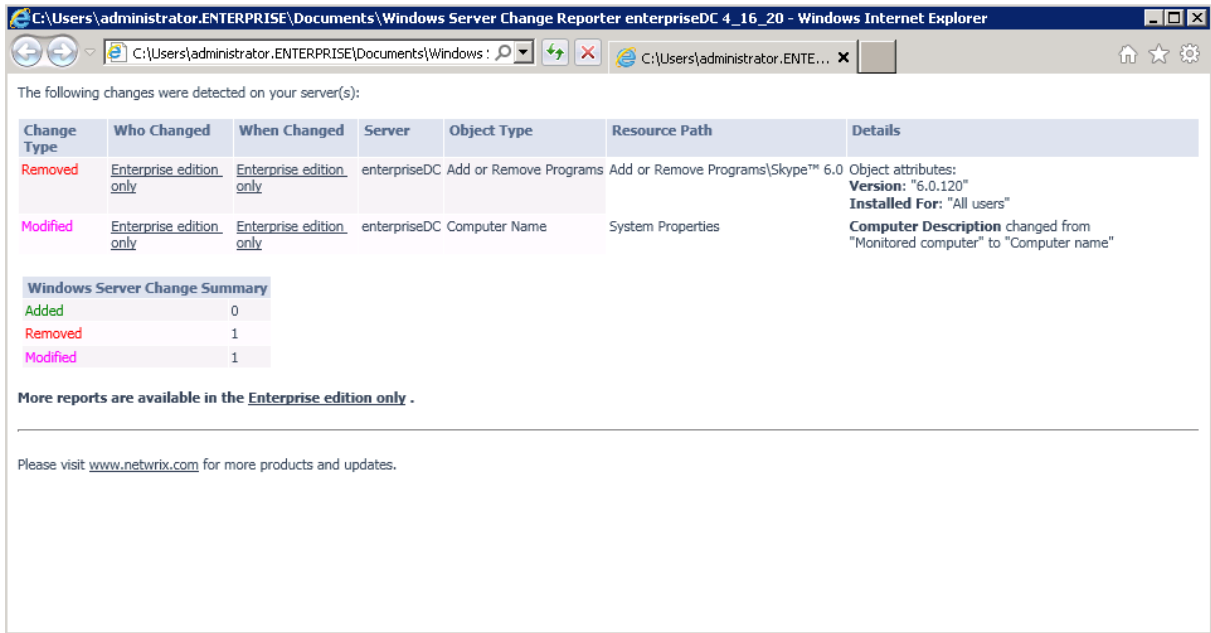
# A    APPENDIX: RELATED DOCUMENTATION

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

*Table 6:    Product Documentation*

| Document Name | Overview |
|---|---|
| Netwrix Windows Server Change Reporter Freeware Edition Quick-Start 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 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 User Guide | 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. |