NETWRIX CHANGE NOTIFIER FOR WINDOWS SERVER

QUICK-START GUIDE

Product Version: 4.0.449

February 2014

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Active Directory is a trademark of Microsoft Corporation. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

Table of Contents

1. INTRODUCTION

1.1. Overview

Netwrix Change Notifier for Windows Server allows automatic tracking of configuration changes made to Windows-based computers. This solution assists in monitoring of all critical systems within the organization, and across multiple sites and Active Directory forests.

Netwrix Change Notifier for Windows Server audits changes in such system components as general computer settings, hardware, software, services, and scheduled tasks.

1.2. Licensing

Netwrix Change Notifier for Windows Server is a freeware product with an unlimited license.

1.3. How It Works

The product data collection and reporting workflow is as follows:

1. An administrator sets the parameters for automated data collection by specifying the Windows servers and their components to be monitored for configuration changes.
2. A dedicated scheduled task which is launched daily collects audit data and writes it to a local file-based storage referred to as Audit Archive.
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. You can also use the Report Viewer tool to generate and view on-demand summaries.

2. Install Netwrix Change Notifier for Windows Server

2.1. Installation Prerequisites

This section provides hardware and software requirements necessary to install Netwrix Change Notifier for Windows Server, and recommendations on how to deploy this product.

2.1.1. Deployment Options

Netwrix Change Notifier for Windows Server can be installed on any computer in the domain to which the monitored servers belong. 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.

Netwrix Change Notifier for Windows Server 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.

2.1.2. Hardware Requirements

Before installing Netwrix Change Notifier for Windows Server, make sure that your hardware meets the following requirements:

Table 1: Netwrix Change Notifier for Windows Server Hardware Requirements

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

- **These are rough estimations. The actual required memory size depends on the average number of changes per day in the monitored environment.**

2.1.3. Software Requirements

Before installing Netwrix Change Notifier for Windows Server, make sure that your system meets the following software requirements:

Table 2: Netwrix Change Notifier for Windows Server Software Requirements

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

2.1.4. Target Server Requirements

The following requirements apply to the monitored servers:

Table 3: Target Server Requirements

Component	Requirement
Operating System	Windows XP or above
Framework	.NET Framework 2.0, 3.0 or 3.5 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.

2.2. Install Netwrix Change Notifier for Windows Server

To install Netwrix Change Notifier for Windows Server, download and run the Netwrix_Change_Notifier_for_Windows_Server.msi file. Follow the instructions of the installation wizard. When prompted, accept the license agreement and specify the installation folder.

3. CONFIGURE RIGHTS AND PERMISSIONS

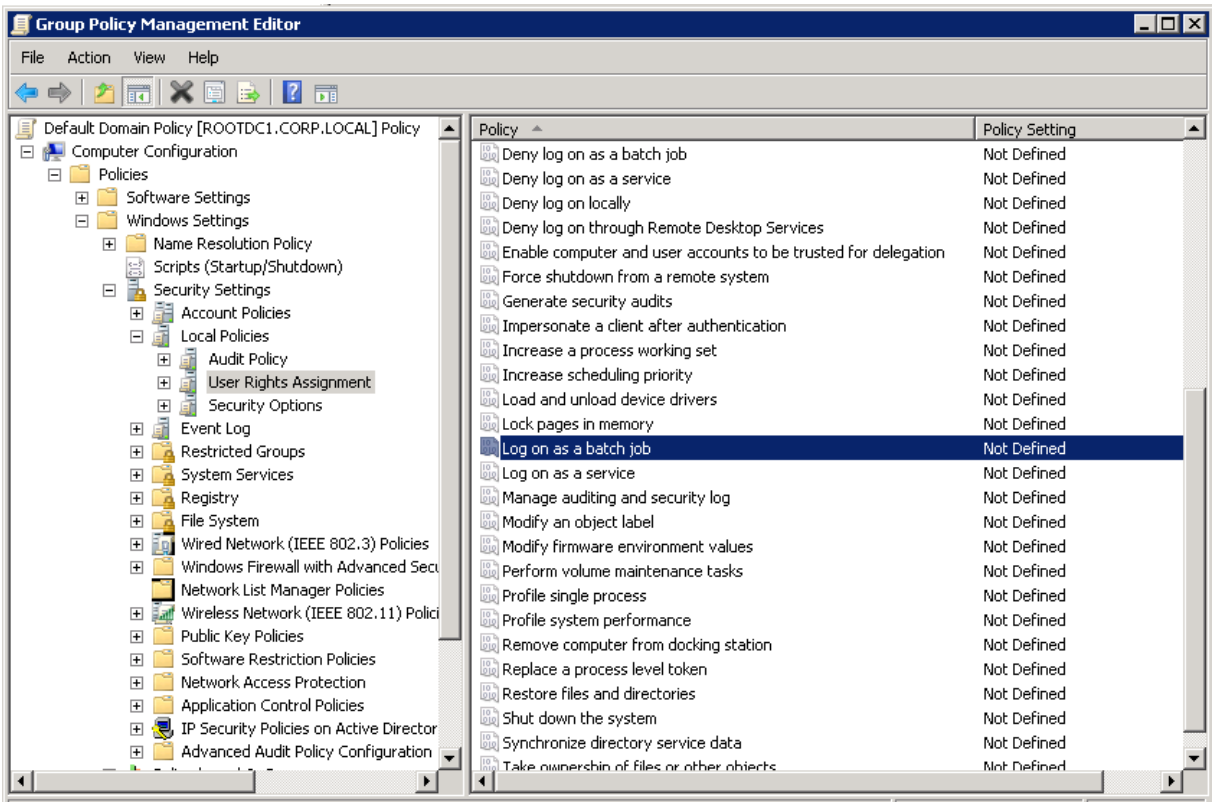
The account under which Netwrix Change Notifier for Windows Server collects data from the monitored servers must have the following rights and permissions:

- The account must be a member of the **Local Administrators group** on the computer where the product is installed and on the target servers.
- The **Log on as a batch job** policy must be defined for this account (see Procedure 1 To define the Log on as a batch job policy)
- The account must be assigned the **Manage auditing and security log** right (see Procedure 2 To assign the "Manage auditing and security log" right)

Procedure 1. To define the Log on as a batch job policy

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

Figure 1: Group Policy Management Editor



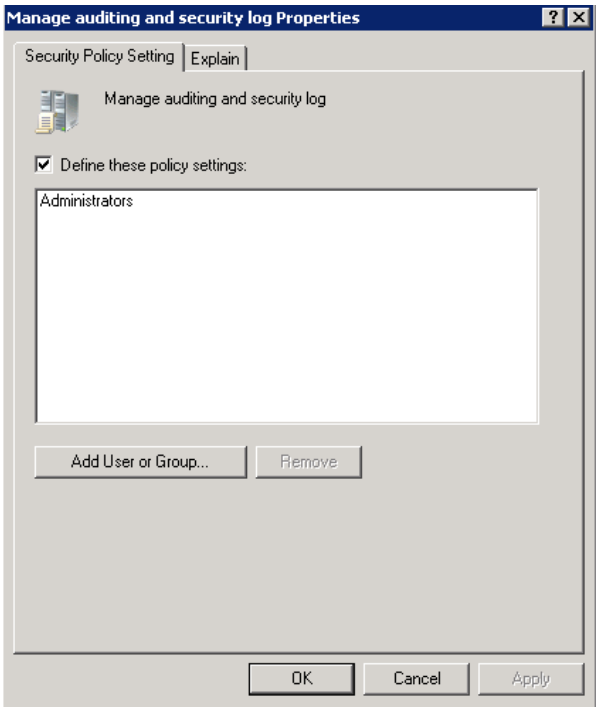
4. Double-click this policy, select **Define these policy settings** and click **Add User or Group**. Specify the account that you want to define this policy for.

5. Navigate to **Start → Run** and type `cmd`. Input the gpupdate /force command and click **Enter** to update the group policy.

Procedure 2. To assign the "Manage auditing and security log" right

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

Figure 2: Manage Auditing and Security Log Properties Dialog



6. Select the **Define these policy settings** option and click the **Add User or Group** button. In the dialog that appears, type in the name of the user that you want to grant this right to and click **OK**.
7. Open the command line interface: navigate to **Start** and type "`cmd`".
8. Type the "`gpupdate /force`" command and press **Enter**. The group policy will be updated.

4. CONFIGURE AUDIT SETTINGS

To collect full audit data, you need to configure Windows Registry audit permissions.

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

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

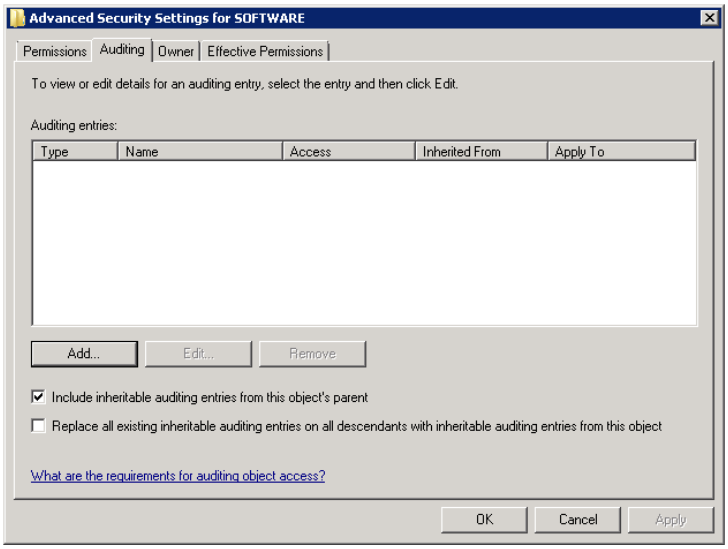
The procedures below provide you with the instructions on how to configure Windows Registry audit permissions, depending on your Windows OS versions:

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

Procedure 3. To configure Windows registry audit settings on pre-Windows Server 2012

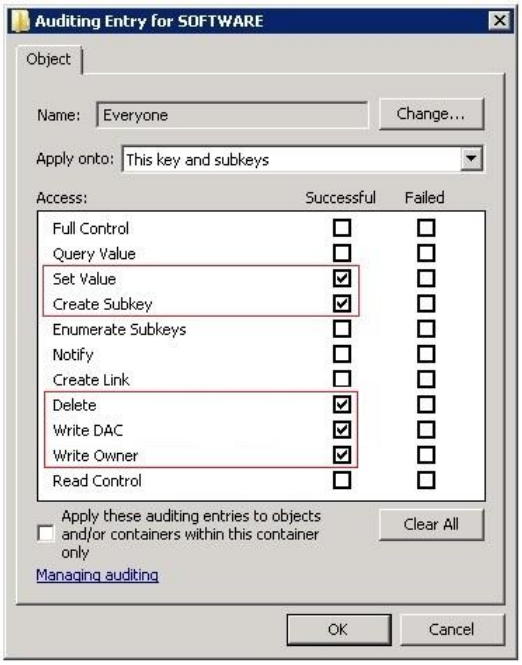
1. On your target server, open **Registry Editor**: navigate to **Start → Run**, enter "regedit" and click **OK**.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** node, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click the **Advanced** button.
4. In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.

Figure 3: Advanced Security Settings for SOFTWARE



5. In the dialog that opens, select the **Everyone** group, and click **OK**.
6. In the Auditing Entry for SOFTWARE dialog, select **Successful** for the following access types: Set Value, Create Subkey, Delete, Write DAC, and Write Owner:

Figure 4: Auditing Entry for SOFTWARE

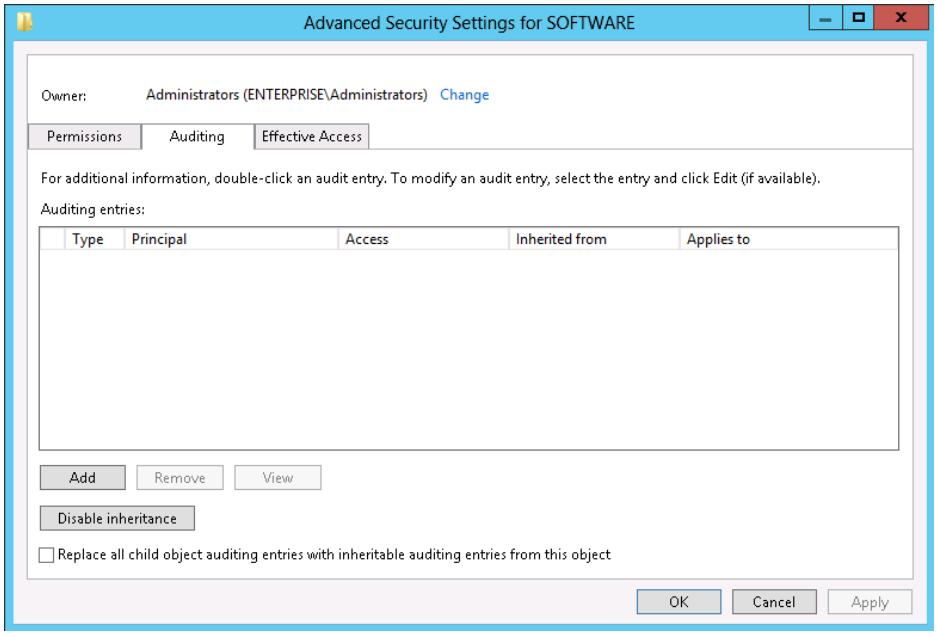


7. Click **OK** and save all changes.
8. Repeat steps 2 to 7 for the HKEY_LOCAL_MACHINE\SYSTEM and HKEY_USERS\.DEFAULT nodes.

Procedure 4. To configure Windows registry audit settings on Windows Server 2012

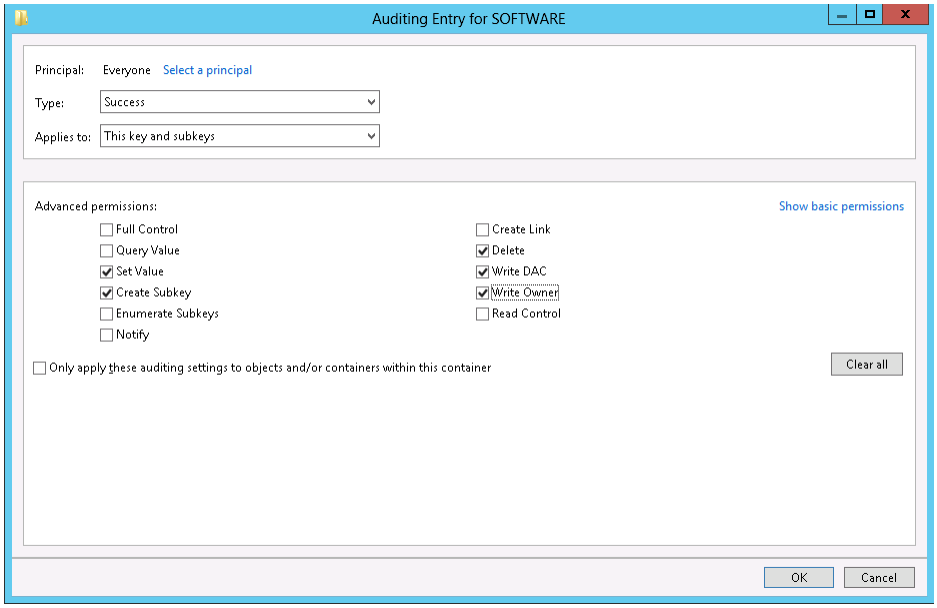
1. On your target server, open **Registry Editor**: navigate to **Start**, type "regedit" and select **regedit** from the Results list.
2. In the registry tree, expand the **HKEY_LOCAL_MACHINE** node, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.
3. In the **Permissions for SOFTWARE** dialog, click the **Advanced** button.
4. In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click the **Add** button.

Figure 5: Advanced Security Settings for SOFTWARE



5. In the dialog that opens, click the **Select a principal** link, enter the **Everyone** group in the **Enter the object name to select** field, and click **OK**.
6. Set the access type to **Successful** and the **Applies to** value to **This key and subkeys**.
7. Click the **Show advanced permissions** link and select the following access types: Set Value, Create Subkey, Delete, Write DAC, and Write Owner:

Figure 6: Auditing Entry for SOFTWARE



8. Click **OK** and save all changes.
9. Repeat steps 2 to 8 for the HKEY_LOCAL_MACHINE\SYSTEM and HKEY_USERS\.DEFAULT nodes.

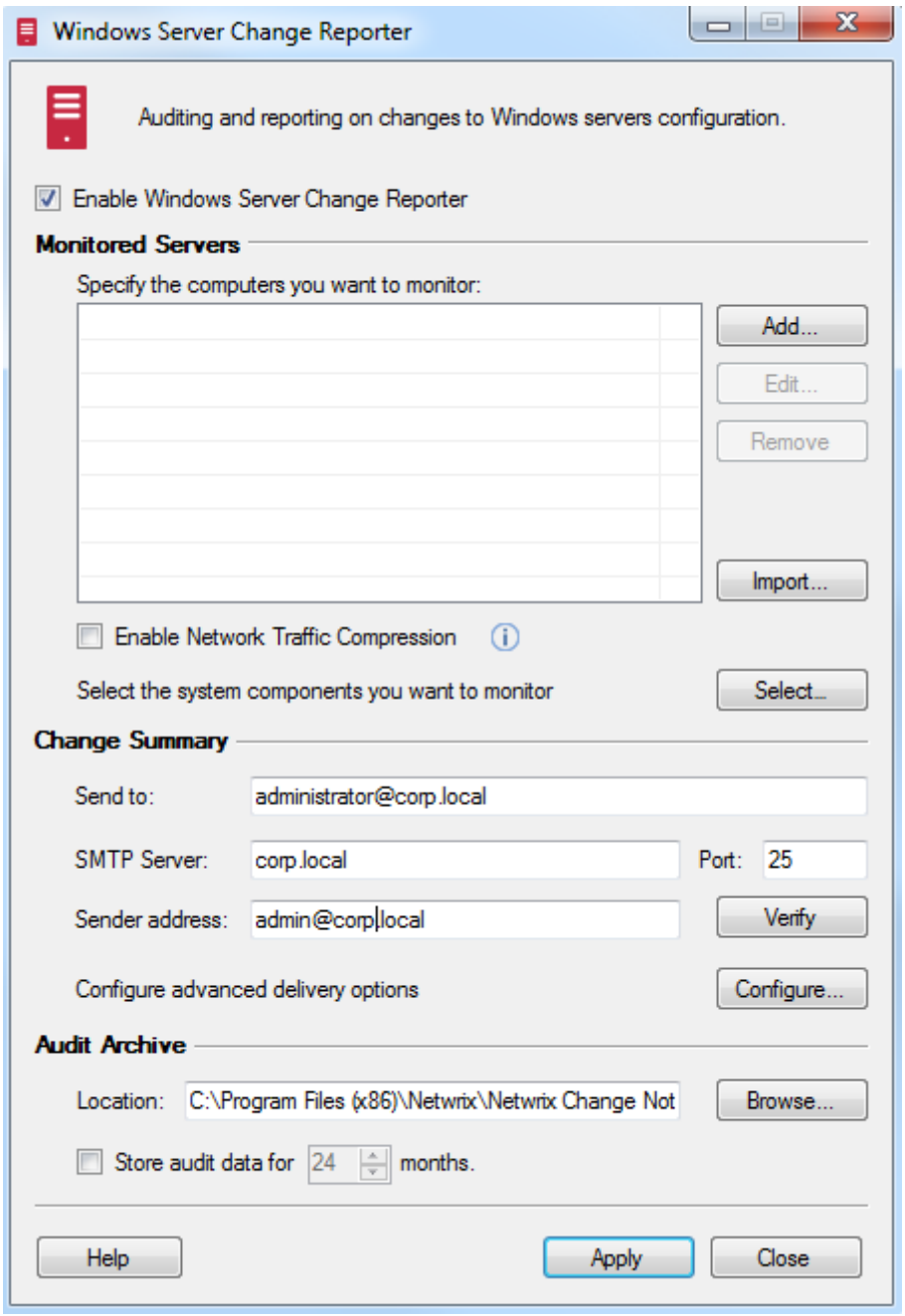
5. Configure Netwrix Change Notifier for Windows Server

After Netwrix Change Notifier for Windows Server has been installed, you need to enable and configure Windows Server audit.

Procedure 5. To Configure Windows Server Audit

1. Navigate to **Start → All Programs → Netwrix Freeware → Netwrix Change Notifier for Windows Server**. The product configuration dialog will open:

Figure 7: The Netwrix Change Notifier for Windows Server Configuration Dialog



2. Specify the following settings and parameters:

Table 4: Netwrix Change Notifier for Windows Server Settings

Parameter	Instruction
Enable Windows Server Change Reporter	Enable this option to start Windows Server audit.
Monitored Servers	
Specify the computers you want to monitor	Click **Add** and enter the names of the computers you want to monitor for configuration changes.
Enable Network Traffic Compression	Enable this option to use agent-based data collection methods. This option is recommended for distributed multi-sites networks or slow connections.
Select the system components you want to monitor	Click **Select** to specify the system components that you wish to monitor for changes. **Note:** Only a limited number of components is available in Netwrix Change Notifier for Windows Server. To monitor other system components, you need to purchase Netwrix Auditor for Windows Server.
Change Summary	
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.
Sender address:	Enter the email address that will appear in the "From" file in the Change Summary emails.
Verify	Click to check your email settings. The product will send a test message to the specified recipients and will inform you if any problems are detected.
Configure advanced delivery options	Click the **Configure** button to modify Change Summary delivery schedule. **Note**: Before you can modify the Change Summary delivery schedule, you must save your current configuration.
Audit Archive	
Location	Specify the location for the local file-based storage of 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 audit data. Make sure that this account has the necessary rights and permissions (see Chapter 3 Configure Rights and Permissions)
5. Enter and confirm the account password and click **OK**.

Note: To modify the product settings later, launch the product configuration dialog from the **Start** menu.

6. Monitor Windows Servers for Changes

When the product has been configured, it starts collecting data on Windows Server changes from the monitored computers. By default, the data collection task is launched daily at 3:00 AM. If required, you can launch the product scheduled task manually or modify its schedule.

6.1. Launch the Product Task Manually

Procedure 6. To launch the product scheduled task manually:

1. Launch **Task Scheduler**.
2. In the left pane, expand the **Task Scheduler Library** node. In the right pane, select the task called ***Netwrix Management Console – Windows Server Change Reporter*.**
3. Right-click the task and select **Run** from the drop-down list. Alternatively, use the **Run** option from the **Actions** menu.

6.2. Modify the Product Task Schedule

Procedure 7. To modify the product task schedule:

1. Launch Netwrix Change Notifier for Windows Server.
2. In the main configuration dialog, click **Configure** next to **Configure advanced delivery options**.
3. In the dialog that opens, click **Change**, modify the default schedule, click **OK**, and click **Apply** in the main window to save the changes.

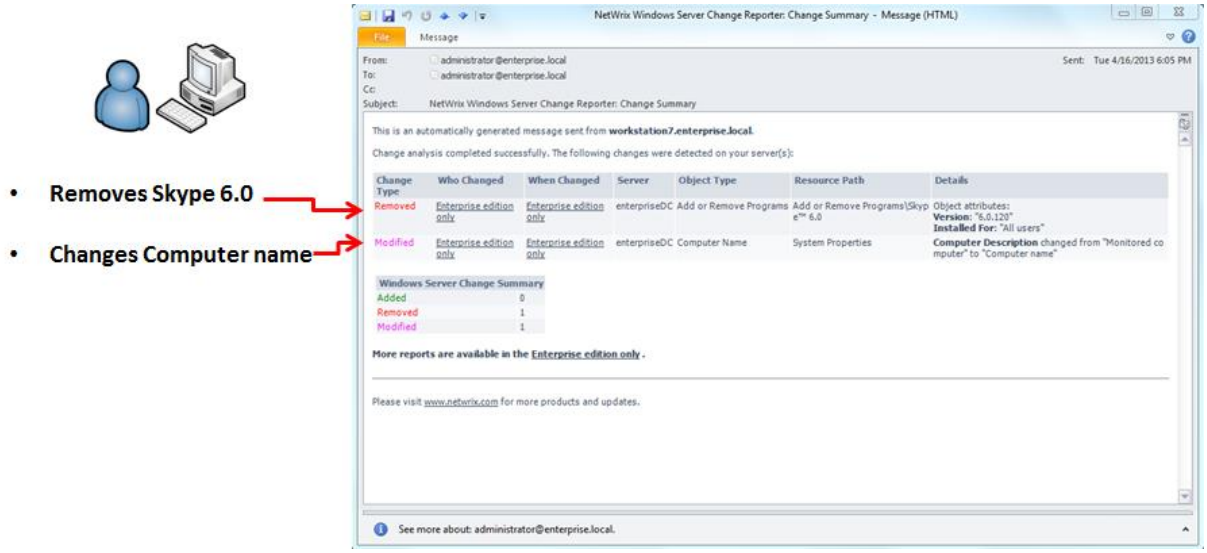
6.3. View a Change Summary

After the first data collection task has finished, an email will be delivered to the specified address notifying you that the initial analysis has been completed.

After that, you can make test changes to your environment to see how they are reported.

When the task is launched the next time (either automatically or manually), it detects the changes made since the last data collection, generates and delivers the Change Summary to the specified recipients:

Figure 8: 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.

6.4. Generate an On-Demand Change Summary

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

Procedure 8. To generate an on-demand Change Summary:

1. Navigate to **Start → All Programs → Netwrix Freeware → Netwrix Change Notifier for Windows Server → Advanced Tools → Report Viewer**.
2. Select the 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.
6. The changes made to server configuration within the specified time frame will be displayed in the default web browser.

Figure 9: Change Summary (Report Viewer)