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.

Table of Contents

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 Netwrix Windows Server Change Reporter Installation and Configuration Guide.

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 and explains its structure.
- Chapter 2 Product Overview 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 3 Netwrix Management Console Overview provides a description of Netwrix Management Console, which is an integrated interface for most Netwrix products.
- Chapter 4 Managed Object explains how to configure a Managed Object. It also explains how to modify Managed Object settings.
- Chapter 5 Data Collection explains the Netwrix Windows Server Change Reporter data collection workflow and contains detailed information on the Change Summary options and Sessions.
- Chapter 6 Reports 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 7 Configuring Global Settings explains how to configure or modify the settings that are applied to all Managed Objects and all Netwrix modules enabled for these objects.
- Chapter 8 Additional Configuration 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.
- A Appendix: Monitored Components and Settings lists all system components and settings monitored by Netwrix Windows Server Change Reporter.
- B Appendix: Related Documentation 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 A Appendix: Monitored Components and Settings.

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 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 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.

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 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 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	Support Forum Knowledge Base	Full range of options: Phone, email, submission of support tickets, Support Forum, Knowledge Base
Licensing	Free of charge	Per server Request a quote

3. NETWRIX MANAGEMENT CONSOLE OVERVIEW

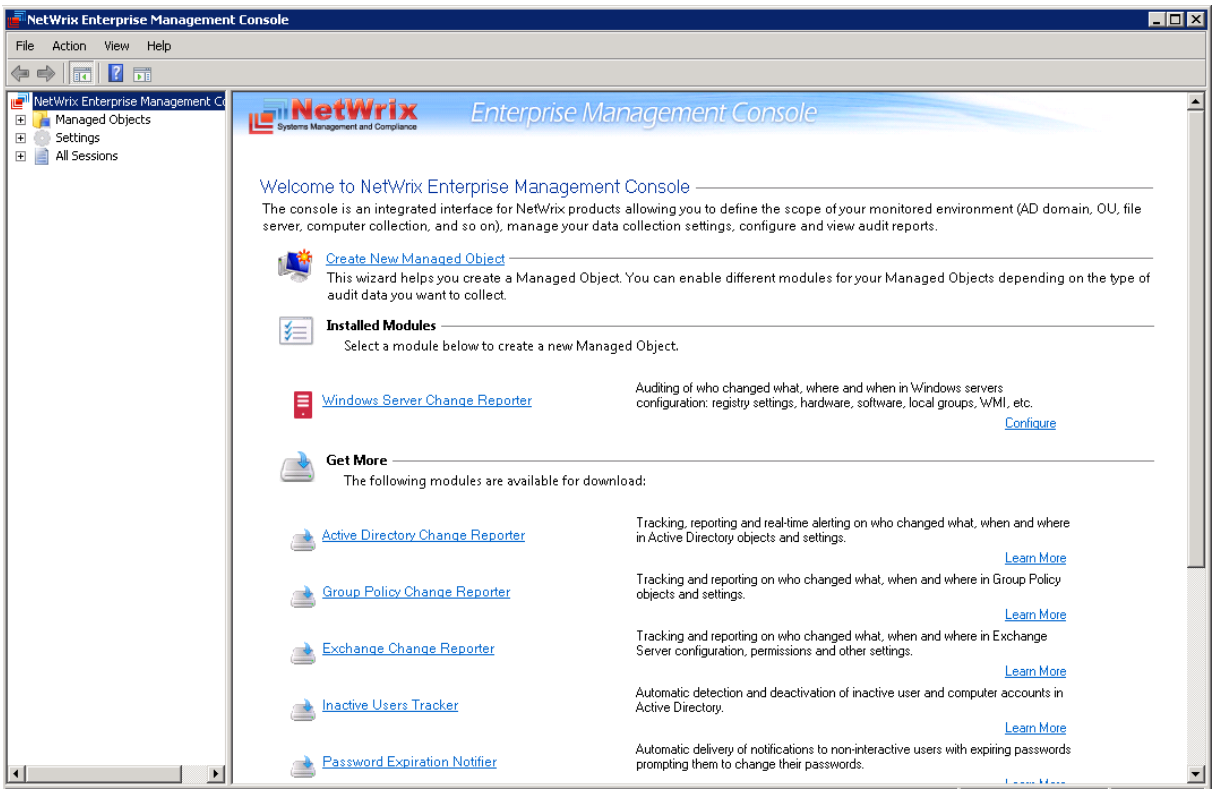
Netwrix Windows Server Change Reporter Enterprise Edition is integrated into Netwrix Management Console, an MMC snap-in that allows configuring Managed Objects and their settings, and the reporting options.

Netwrix Management Console enables you to do the following:

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

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

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
- Modify Managed Object settings

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:

Figure 2: Managed Objects Page

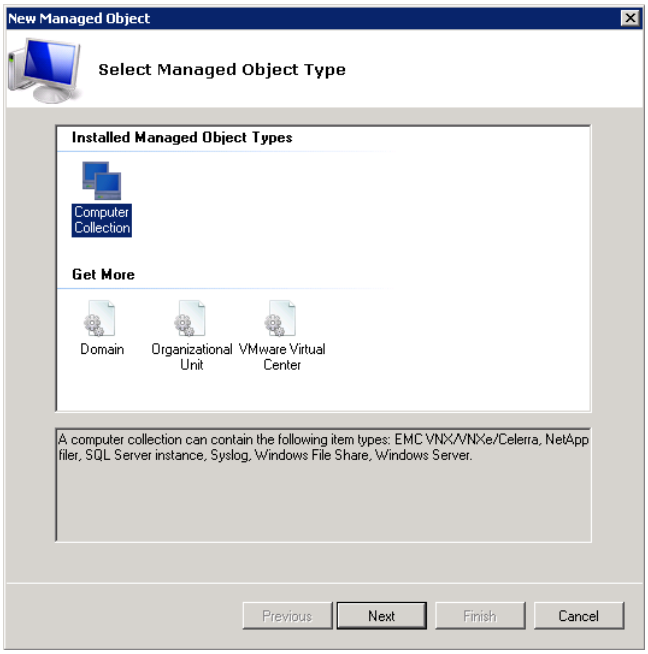
2. Click **Create New Managed Object** in the right pane. Alternatively, right-click the **Managed Objects** node and select **New Managed Object** from the popup menu to start the **New Managed Object** wizard.

   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.

Figure 3: New Managed Object: Select Managed Object Type



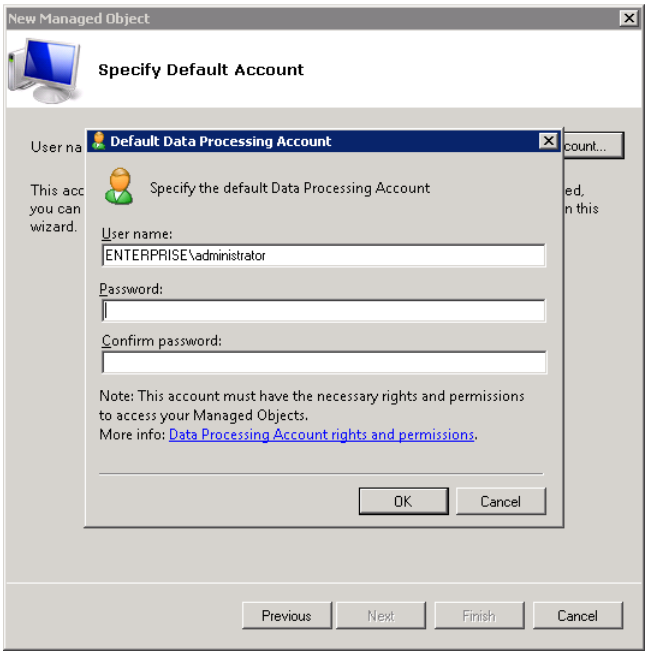
4. On the **Specify Default Account** step, click the **Specify Account** button.

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 NetWrix Windows Server Change Reporter Installation and Configuration Guide.
- 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 NetWrix Windows Server Change Reporter 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 NetWrix Windows Server Change Reporter Installation and Configuration Guide.

Figure 4: New Managed Object: Specify Default Account

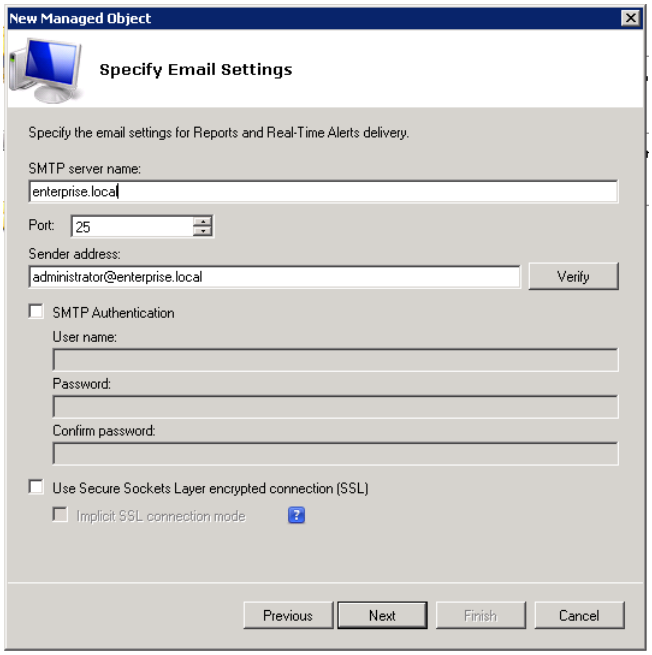


Click **OK** to continue and then **Next**.

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 Procedure 3 To modify the Data Processing Account), or for all Managed Objects in a batch (for instructions, refer to Procedure 22 To configure the Data Collection settings).

5. On the **Specify Email Settings** step, provide the email settings that will be used for Change Summary and Reports delivery:

Figure 5: New Managed Object: Specify Email Settings



The following parameters must be specified:

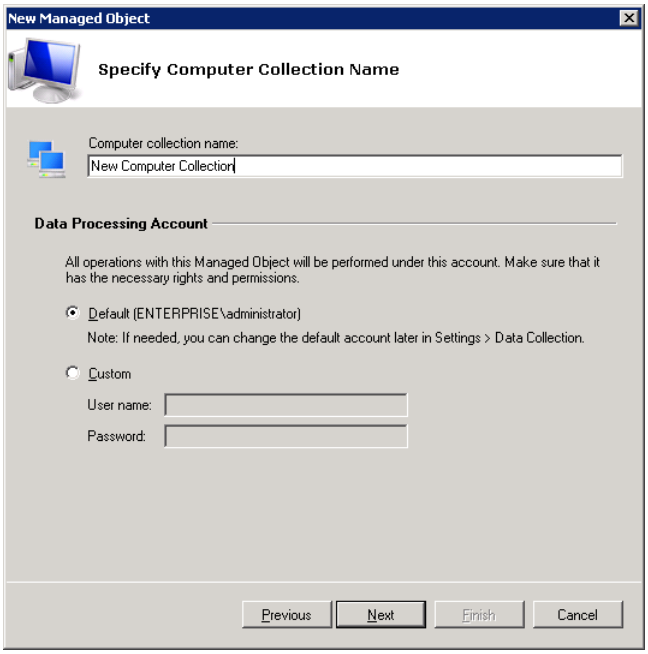
Table 2: Email Settings Parameters

Parameter	Description
SMTP server name	Enter your SMTP server name.
Port	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the 'From' field in Reports and Change Summaries. 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.

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

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

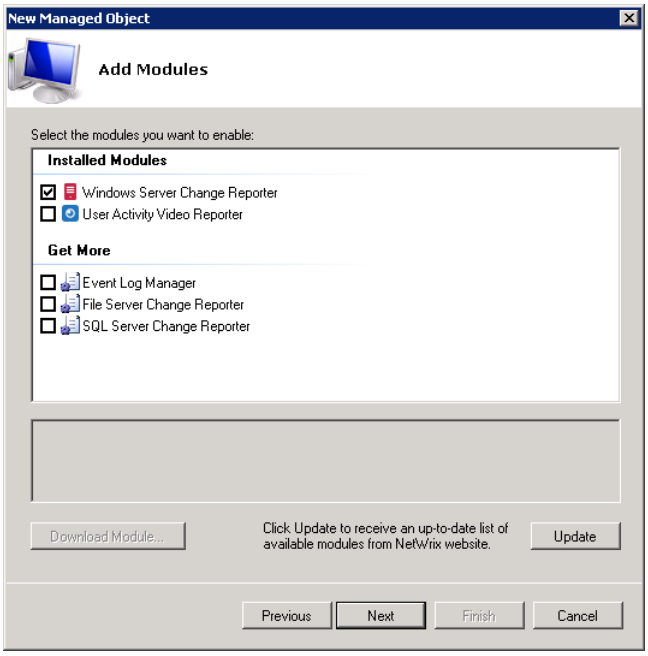
Figure 6: New Managed Object: Specify Computer Collection Name



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**:

Figure 7: New Managed Object: Add Modules

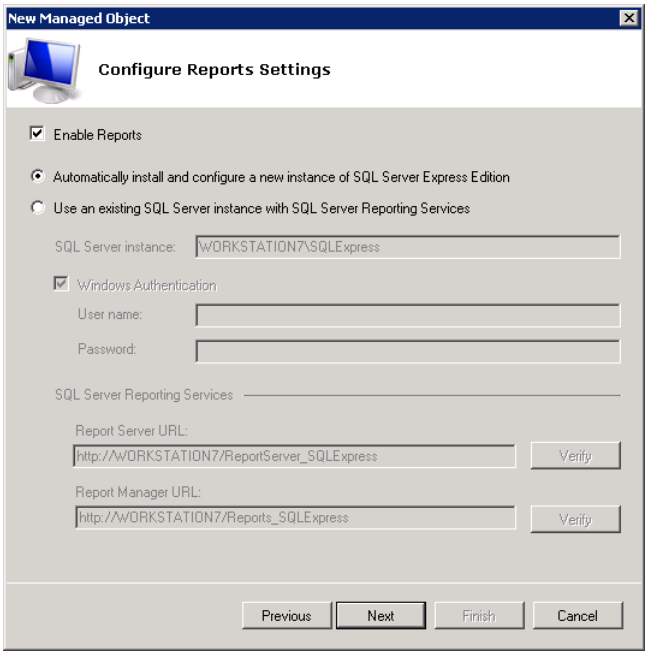


Note: If you have not installed any other Netwrix change reporting products before, this step will be omitted.

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:

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 6.2 Configuring Reports 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:

Table 3: Reports 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 Netwrix Windows Server Change Reporter Installation and Configuration Guide.
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.

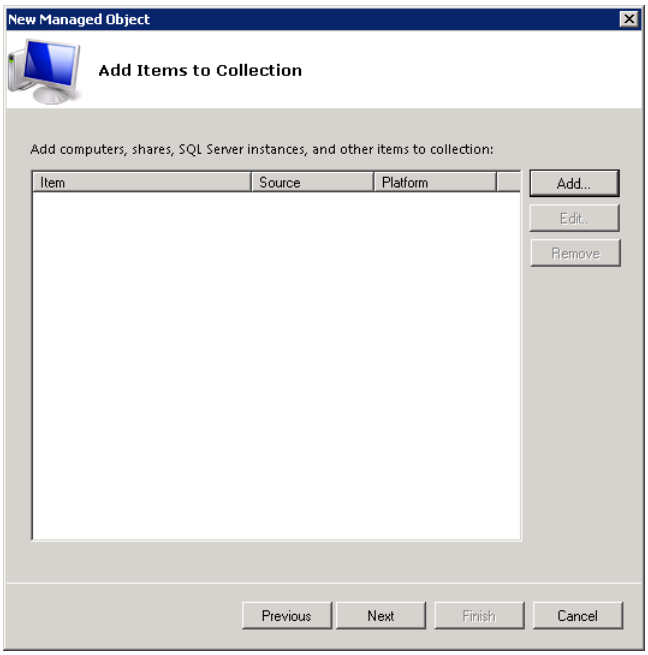
Note: If you already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable the Reports feature. If you want to use custom Reports settings for this Managed Object (for example, write data to a different SQL database),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

Reports settings later (for instructions, refer to Section 6.2.1 Specifying SQL Server Settings 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:

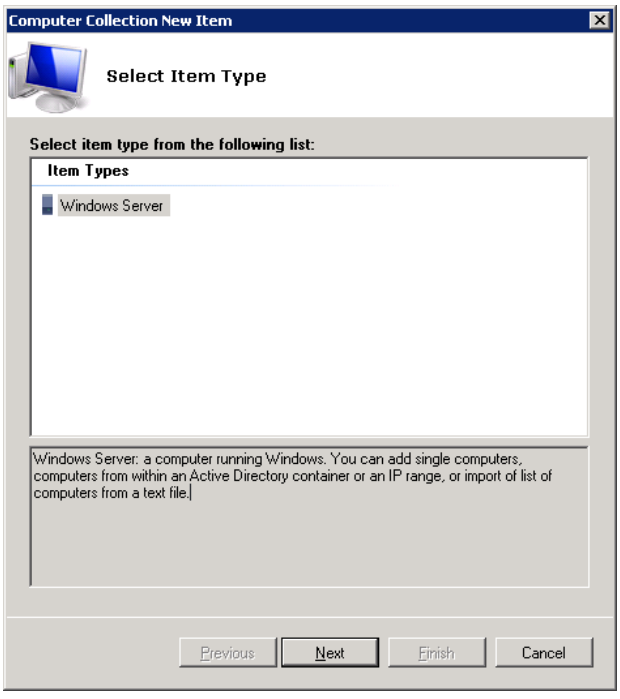
Figure 9: New Managed Object: Add items to Collection



The **Computer Collection New Item** wizard starts.

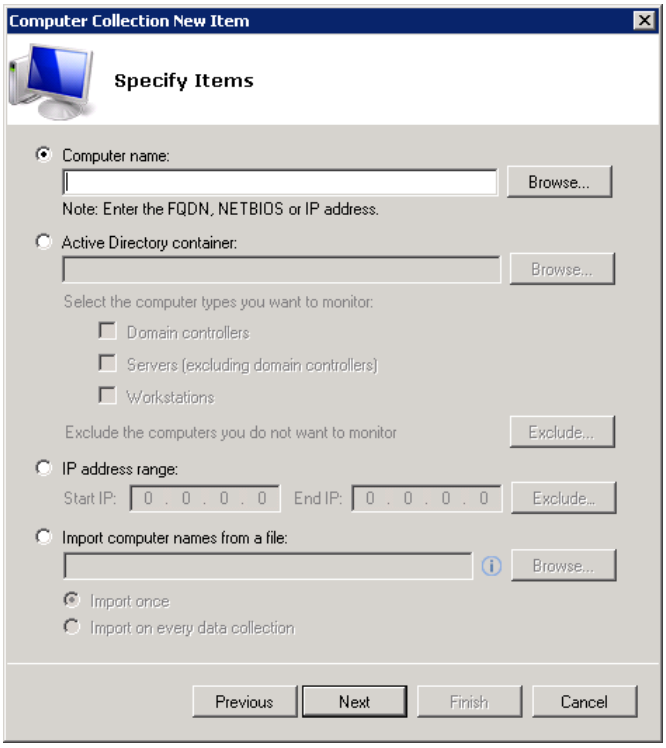
10. On the **Select Item Type** step, select **Windows Server** as the item type, and click **Next** to specify the computers to monitor:

Figure 10: Computer Collection New Item: Select Item Type



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

Figure 11: Computer Collection New Item: Specify Items

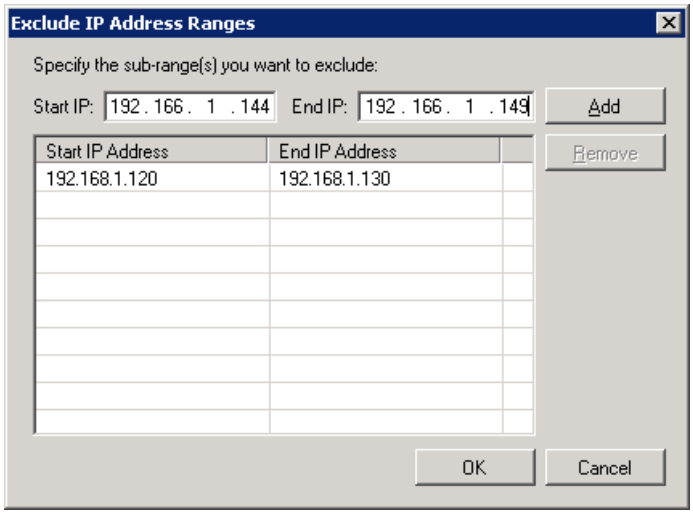


- **Computer name** allows specifying a single computer by entering its FQDN, NETBIOS or IP address. You can click **Browse** to select a computer from the list of computers in your network.
- **Active Directory container** allows specifying a whole AD container. Click **Browse** to select from the list 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.
    - 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**:

Figure 12: Exclude IP Address ranges



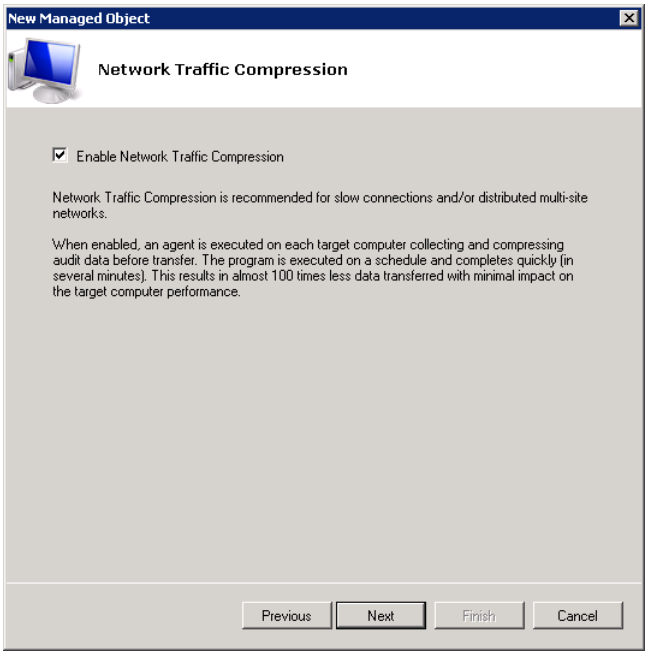
- **Import computer names from a file** allows specifying multiple computer names by importing a list from a `.txt` file (one computer name/IP address per line is accepted). You can choose whether to import the list once, or to update it on every data collection.

  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.

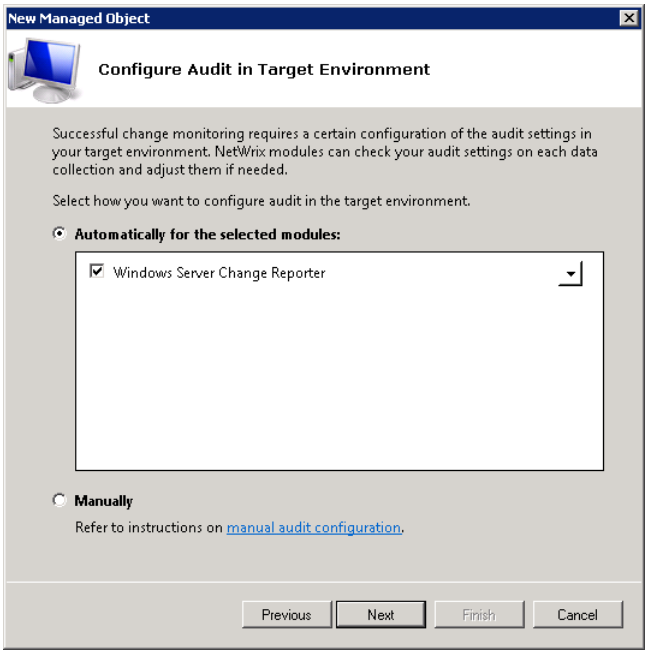
12. On the **Network Traffic Compression** step you can enable the **Network Traffic Compression** option. If this feature is enabled, an agent will be installed automatically on the target servers that will collect and pre-filter data and return it in a highly compressed format. This significantly improves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

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



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:

Table 4: Audit Settings

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
Local Audit Policies	For pre-Vista Windows versions, the following policies are set to "Success": • Audit object access • Audit account management 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".

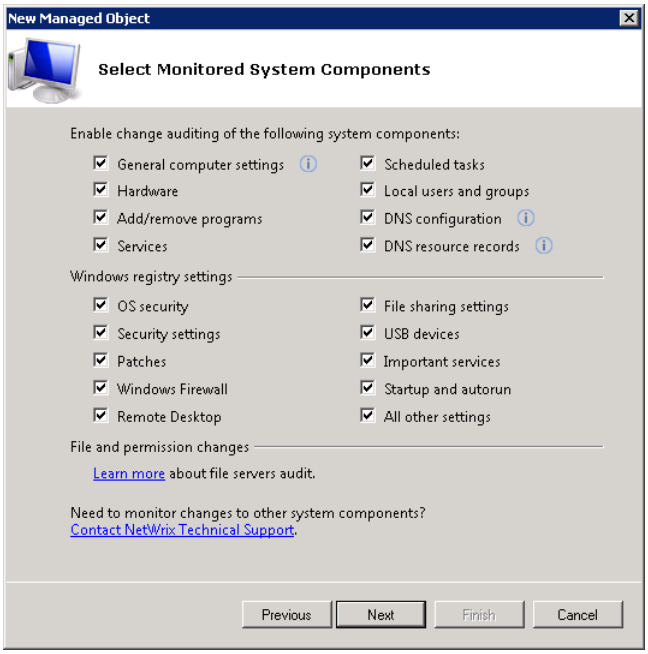
Note: If your target computer is a domain controller, only the Windows registry audit permissions and the event log size with retention method can be configured automatically. Local audit policies need to be configured manually. For instructions on the manual audit configuration, refer to Chapter 5 Configuring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

Automatic audit configuration is performed on every data collection: the product checks the current audit settings and adjusts them to the values specified in Table 4: Audit Settings 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

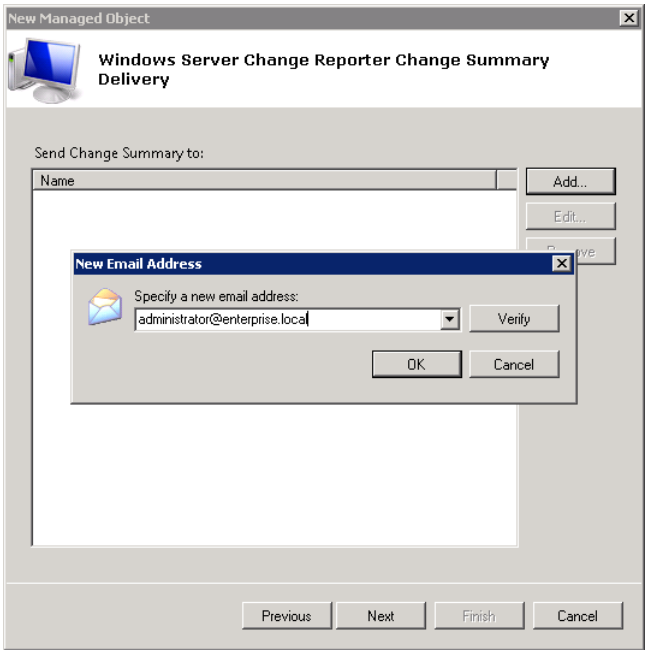


Note: For a full list of monitored components, refer to A Appendix: Monitored Components and Settings.

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):

Figure 16: Widows Server Change Reporter Change Summary Delivery

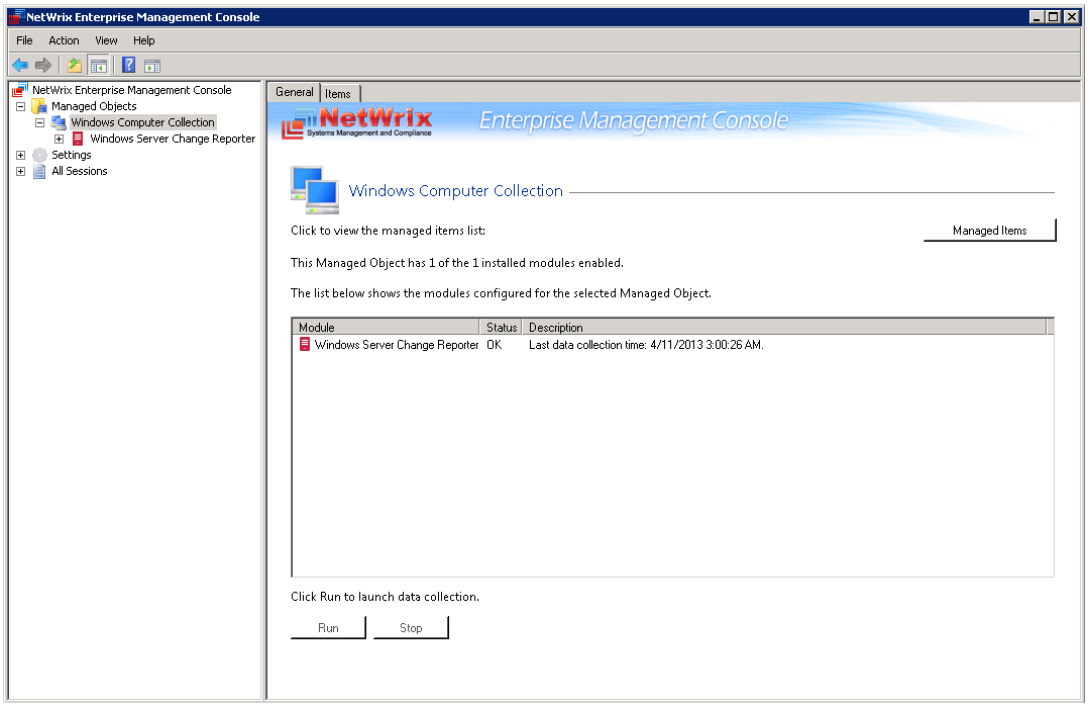


It is recommended to click the **Verify** button. The system will send a test message to the specified email address and will inform you if any problems are detected. Click **OK** to save the changes and then click **Next** to continue.

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:

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:

- To modify general settings: add or remove Netwrix modules for the selected Managed Object.

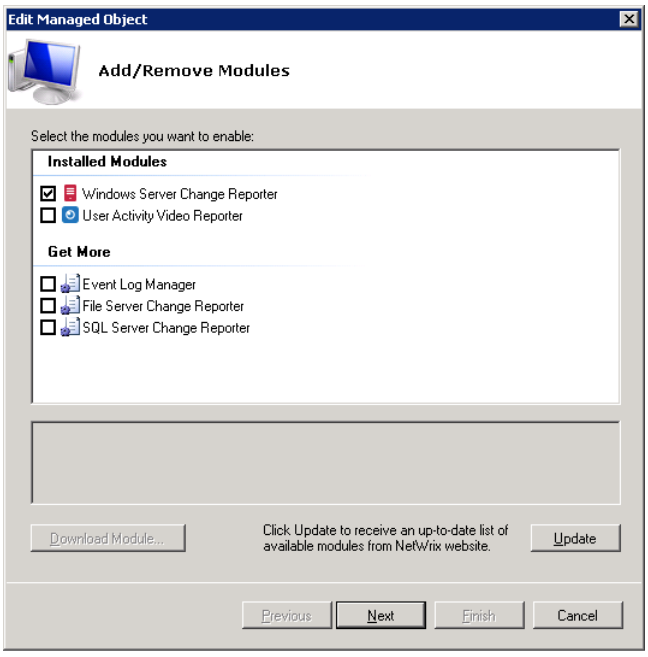
Note: This option is only available if you have already installed other Netwrix change reporting products that have Computer Collection as the managed object type.

- To modify the Data Processing Account: override the Default Data Processing Account for this Managed Object and specify a different account for data collection.
- To add/remove items to/from Computer Collection: add or remove items to/ from Computer Collection.
- To modify Windows Server Change Reporter settings: 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:

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.

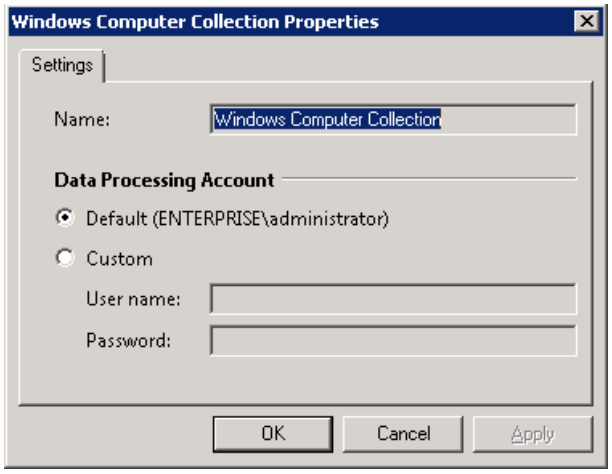
   In this dialog, under **Get More**, there is also a list of other Netwrix products that can have Computer Collection as a Managed Object type. To get more information on

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:

Figure 19: Managed Object Properties

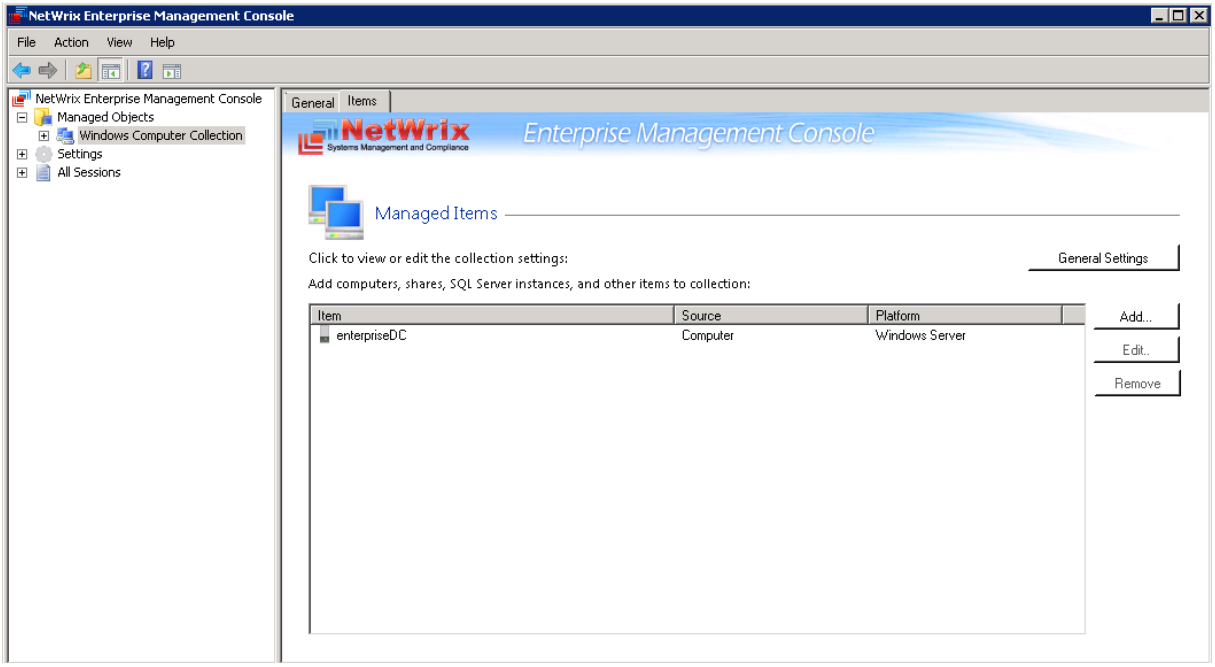


3. Click **OK** to save the changes. This account will be used for data collection from this Managed Object.

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



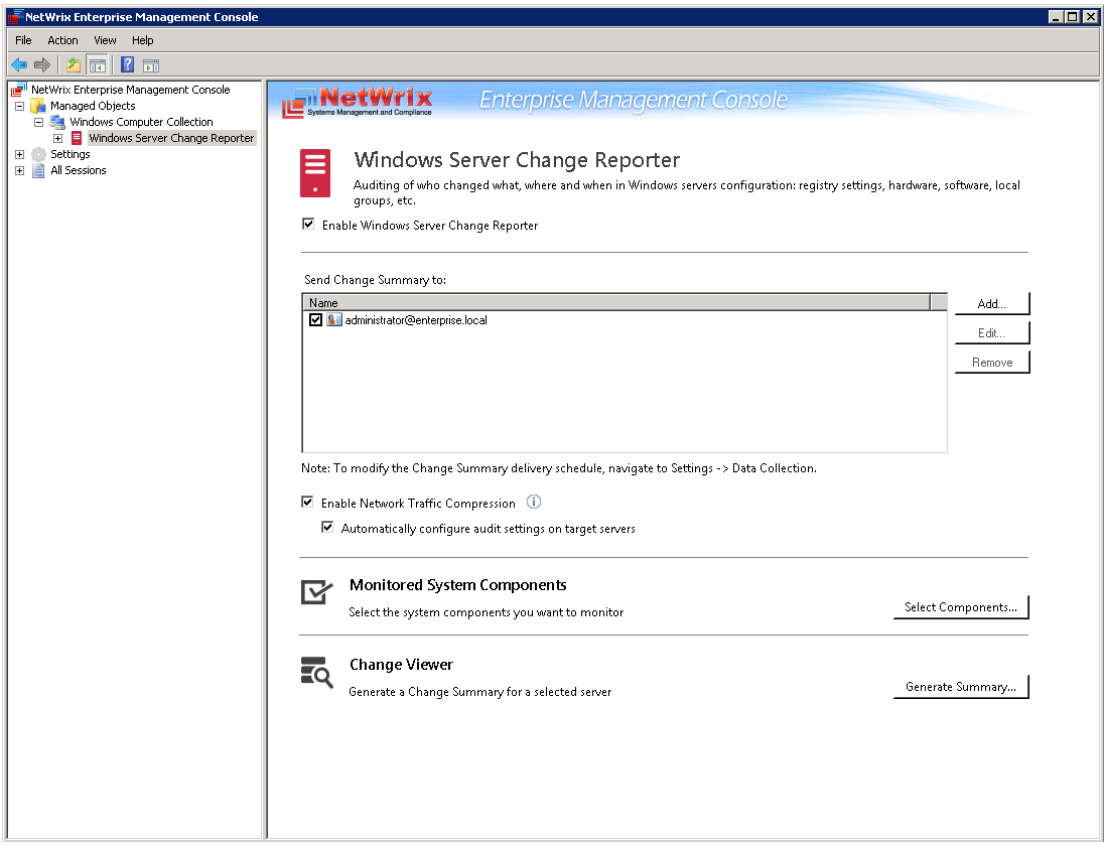
3. Do one of the following:

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

Procedure 5. To modify Windows Server Change Reporter settings

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

Figure 21: Windows Server Change Reporter Page



2. To modify Netwrix Windows Server Change Reporter settings, do the following:

   - To disable (or enable, if disabled) the Windows Server Change Reporter module for this Managed Object, deselect/select the corresponding checkbox.
   - To add an email address to the Change Summary recipients list, 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.
   - To modify an email address in the Change Summary recipients list, select it and click the **Edit** button. Edit the address and click **OK.**
   - To remove an email address from the Change Summary recipients list, select it and click the **Remove** button. The selected address will be deleted.
   - To disable (or enable, if disabled) the Network Traffic Compression option, select/deselect the corresponding checkbox. It is recommended to enable this option, otherwise the collected audit data may be incomplete.
   - To disable (or enable, if disabled) the **Automatically configure audit settings on target servers** option, select/deselect the corresponding checkbox. For a list of the settings that will be configured automatically, refer to Table 4: Audit Settings.
   - To modify the list of the system components you want to monitor, 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 A Appendix: Monitored Components and Settings.

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:

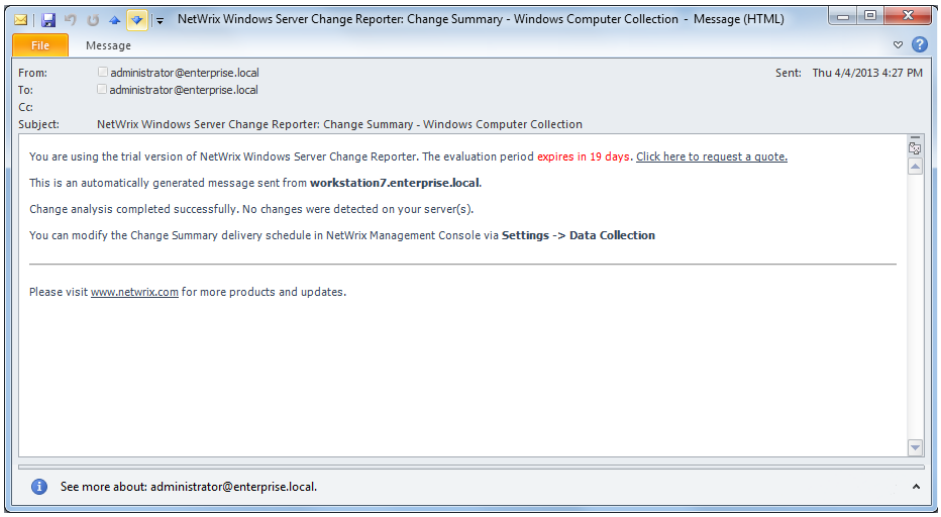
- Data collection workflow
- Change Summary
- Sessions

5.1. Data Collection Workflow

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:

Figure 22: Initial Analysis Notification



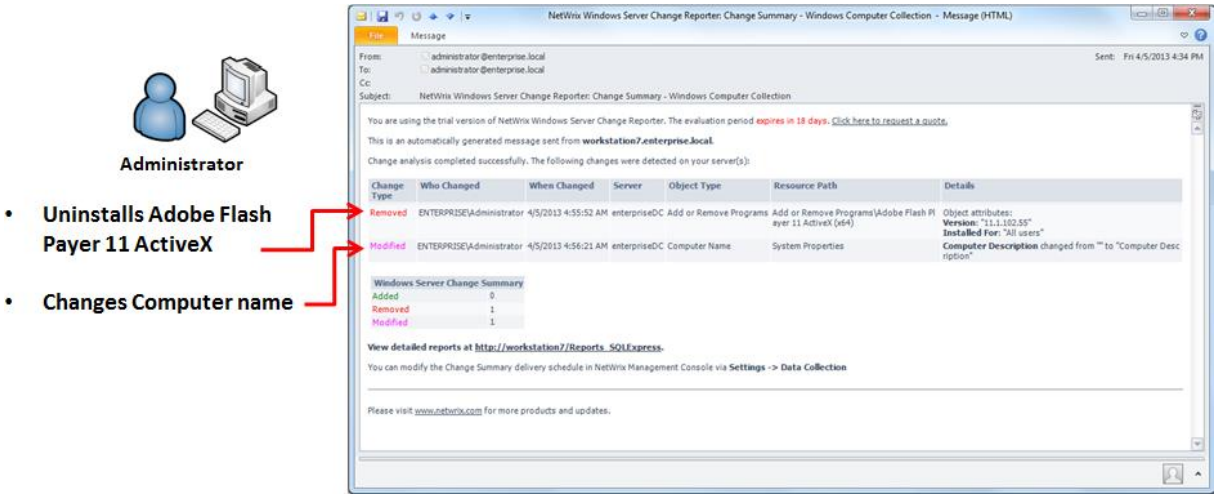
3. When the data collection has been completed, Netwrix Windows Server Change Reporter writes data on the detected changes to a local storage, the Audit Archive. By default, the data collection is performed once a day at 3:00 AM. If the Reports feature is enabled and configured, data is then imported 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 7.4 Configuring Data Collection Settings).

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 Netwrix Windows Server Change Reporter Installation and Configuration Guide.

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:

Figure 23: Change Summary Example



The Change Summary provides the following information for each change:

Table 5: 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.

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

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** → **<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.

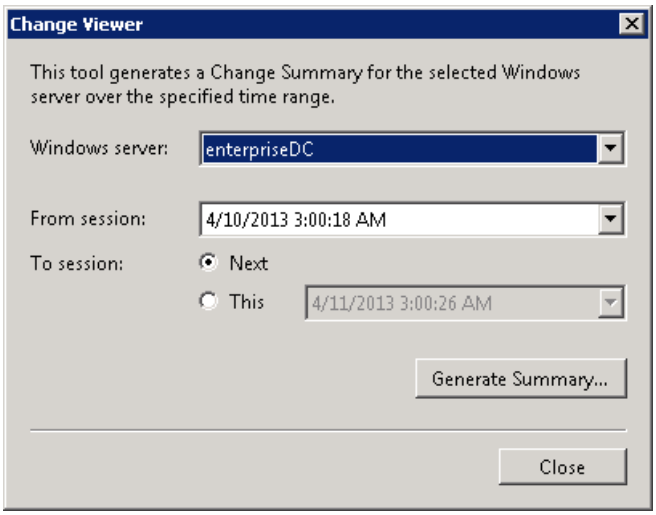
5.2.2. Viewing Change Summary for the Specified Time Frame

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

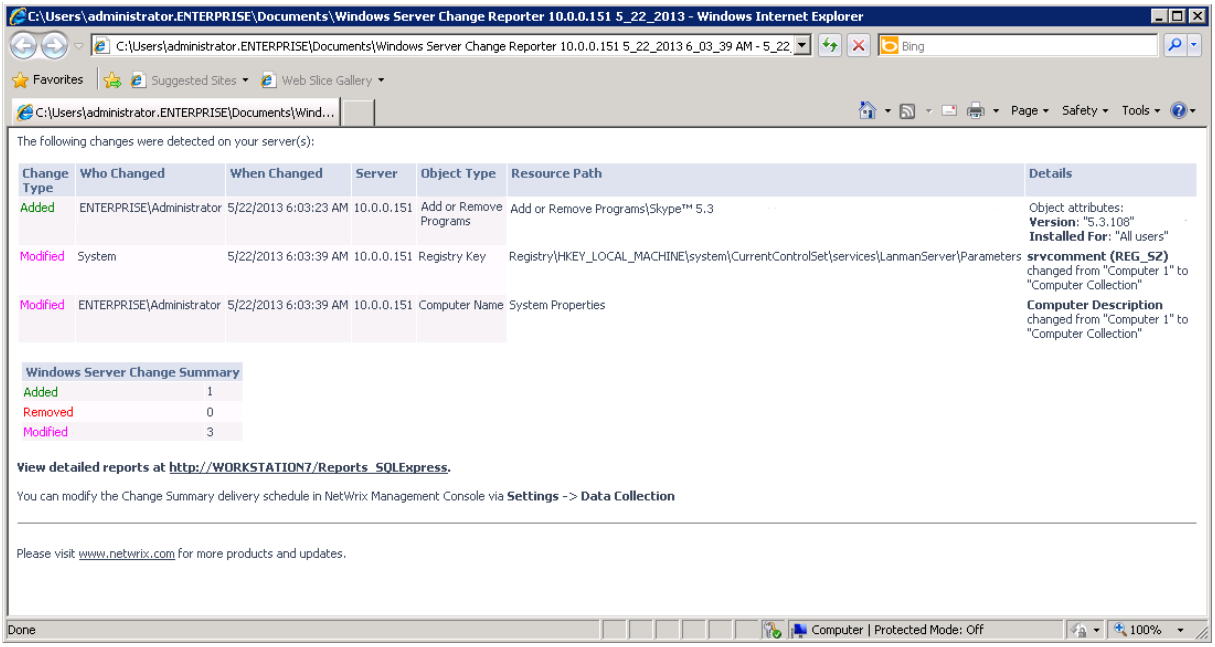
1. In Netwrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** → **Windows Server Change Reporter** (see Figure 21: Windows Server Change Reporter Page).
2. In the right pane, click the **Generate Summary** button next to **Change Viewer**. The Change Viewer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

Figure 24: Netwrix Windows Server Change Reporter Viewer



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

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 Reports functionality to review changes made to the monitored domain.

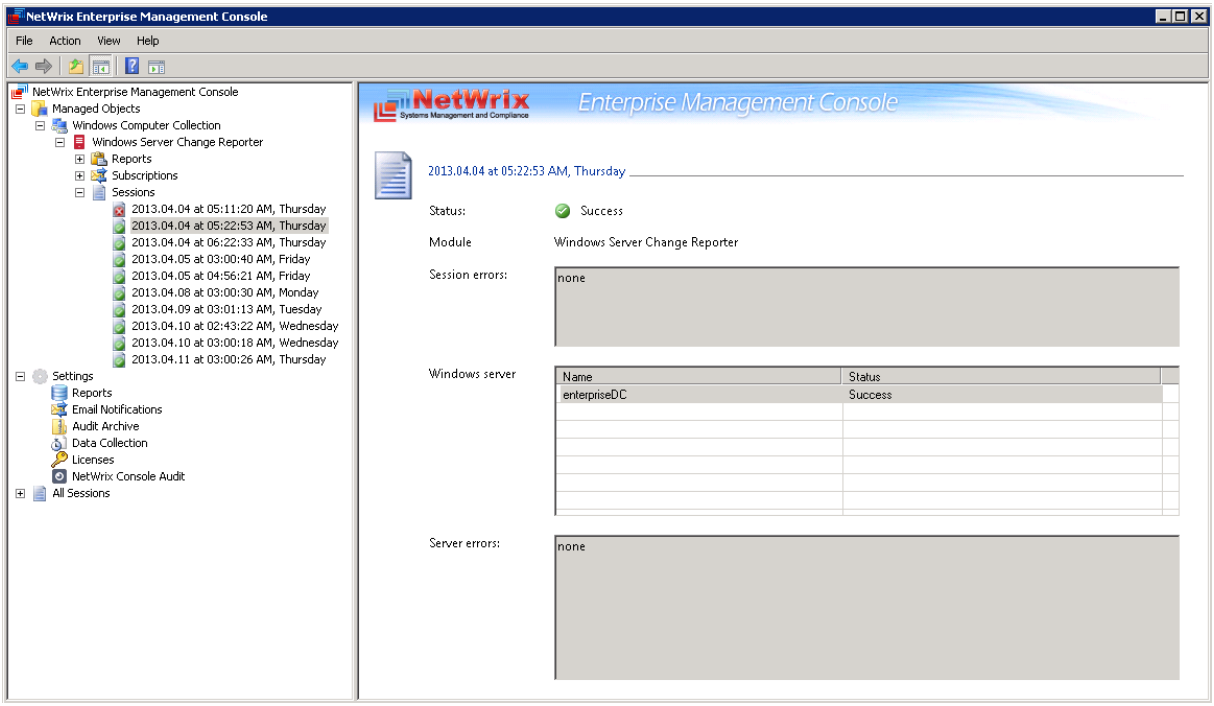
5.3. Sessions

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

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

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 7.3 Configuring Audit Archive Settings.

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.

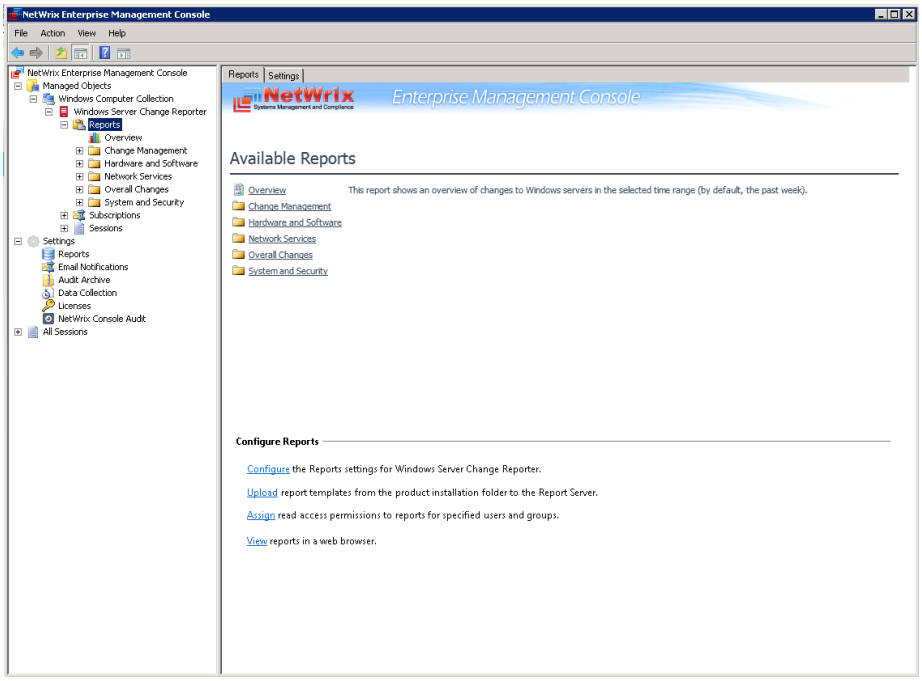
> **Note:** If your situation requires the use of additional report types, you can order custom report templates from Netwrix.

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

- Overview: 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 6.5 Overview Report.
- Change Review History: 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 6.6 Change Management.
- Change Reports: 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 → <Managed_Object_name> → Windows Server Change Reporter → Reports**:

Figure 27: Reports



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
- Assign permissions to view web-based reports

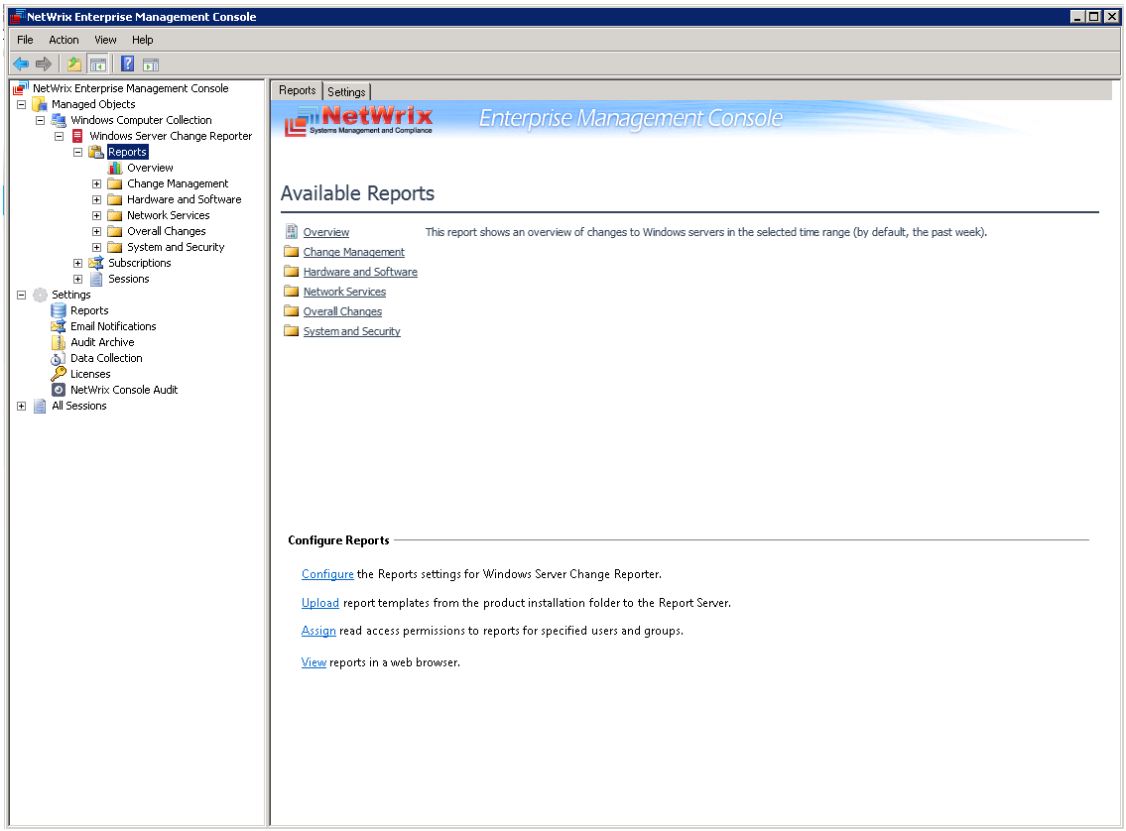
6.2.1. Specifying SQL Server Settings

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

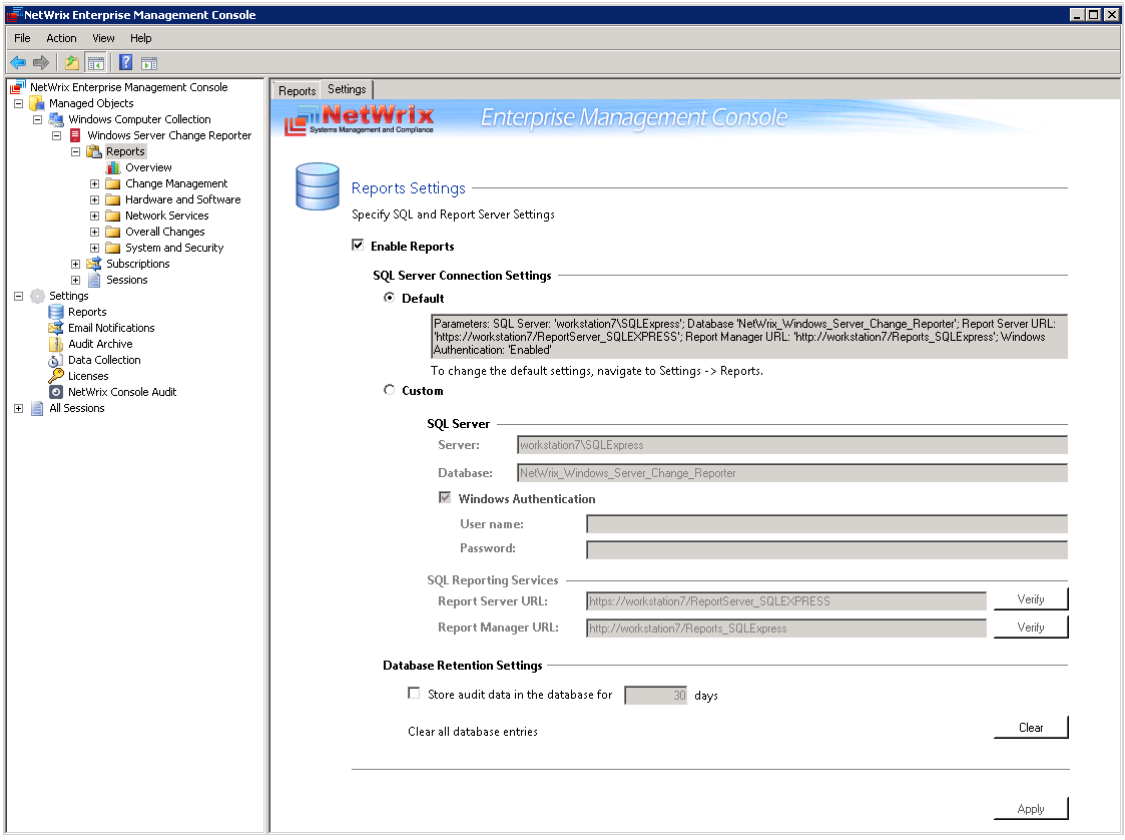
1. In Netwrix Enterprise Management Console, expand the **Managed Object** → **<Managed_Object_name>** → **Windows Server Change Reporter** node and select **Reports**. The following page will be displayed:

Figure 28: Reports Page



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

Figure 29: Reports Settings



3. Specify/modify the following parameters:

Table 7: Reports Settings

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 Netwrix Windows Server Change Reporter Installation 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.
Clear all database entries	Click the **Clear** button if you want to delete all data from the SQL database. **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: Error: A transport-level error has occurred when sending the request to the server.

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:

- Upload the report templates to the Report Server (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 6.2.2 Uploading Report Templates to the Report Server.
- Import audit data to the SQL database. 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 6.2.3 Importing Audit Data to SQL Database.

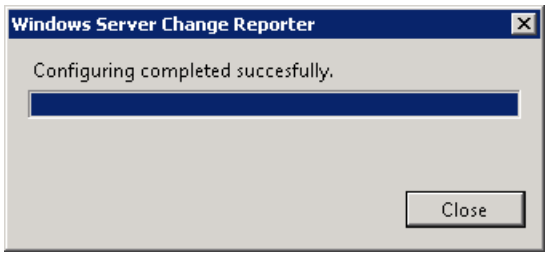
6.2.2. Uploading Report Templates to the Report Server

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 Figure 28: Reports Page), 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 Templates



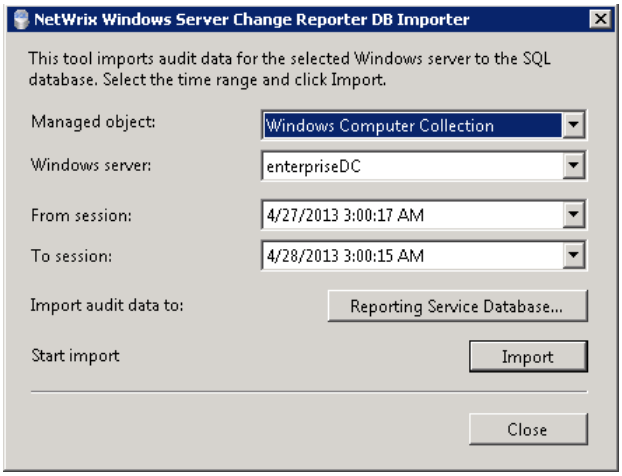
6.2.3. Importing Audit Data to SQL Database

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

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

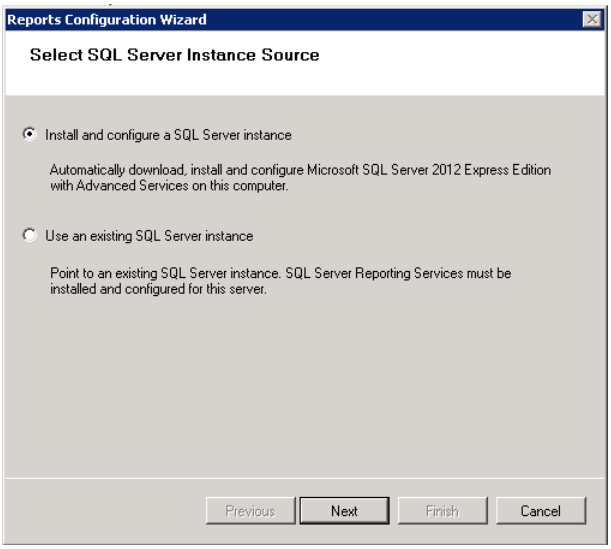
Figure 31: Netwrix DB Importer



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:

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.

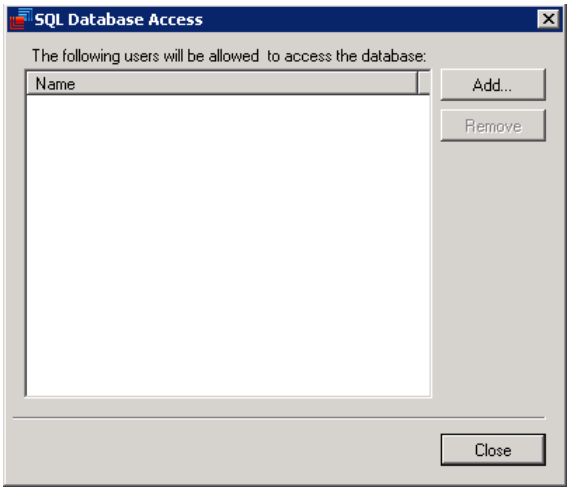
6.2.4. Assigning Permissions to View Reports

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 Figure 28: Reports Page), click **Assign** under **Configure Reports**. The following dialog will be displayed:

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:

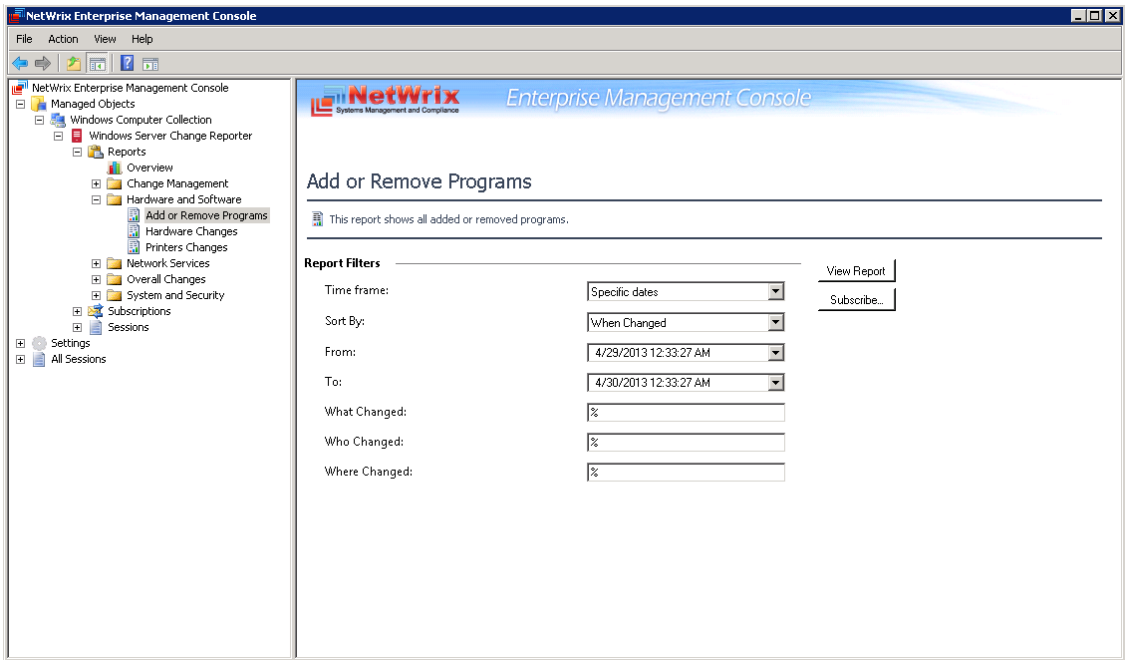
- In Netwrix Management Console
- In a web browser

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 → <Managed_Object_name> → Windows Server Change Reporter → 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):

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:

Figure 35: Add or Remove Programs Report (Console)

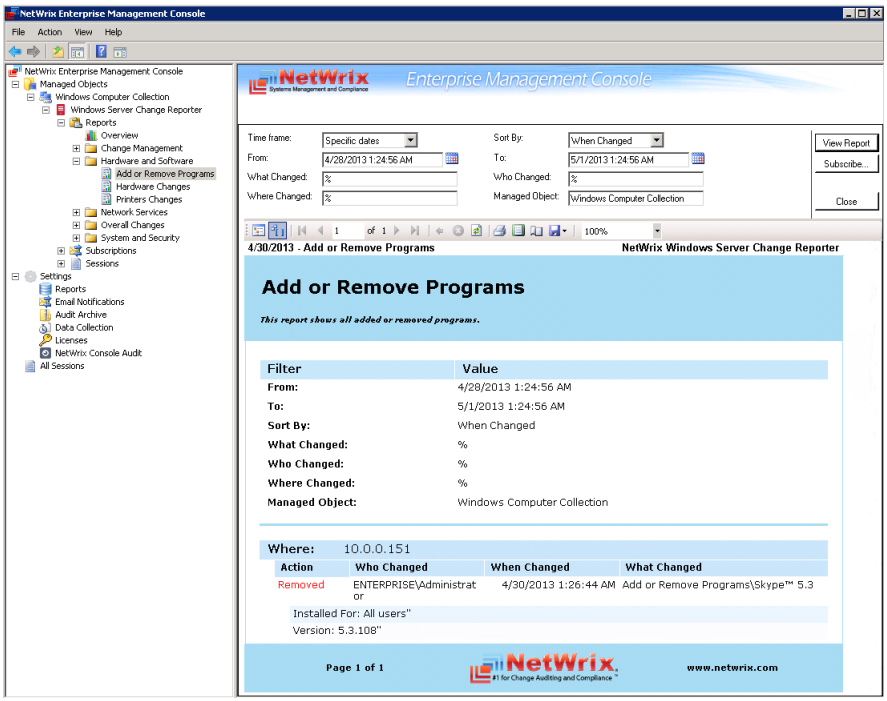
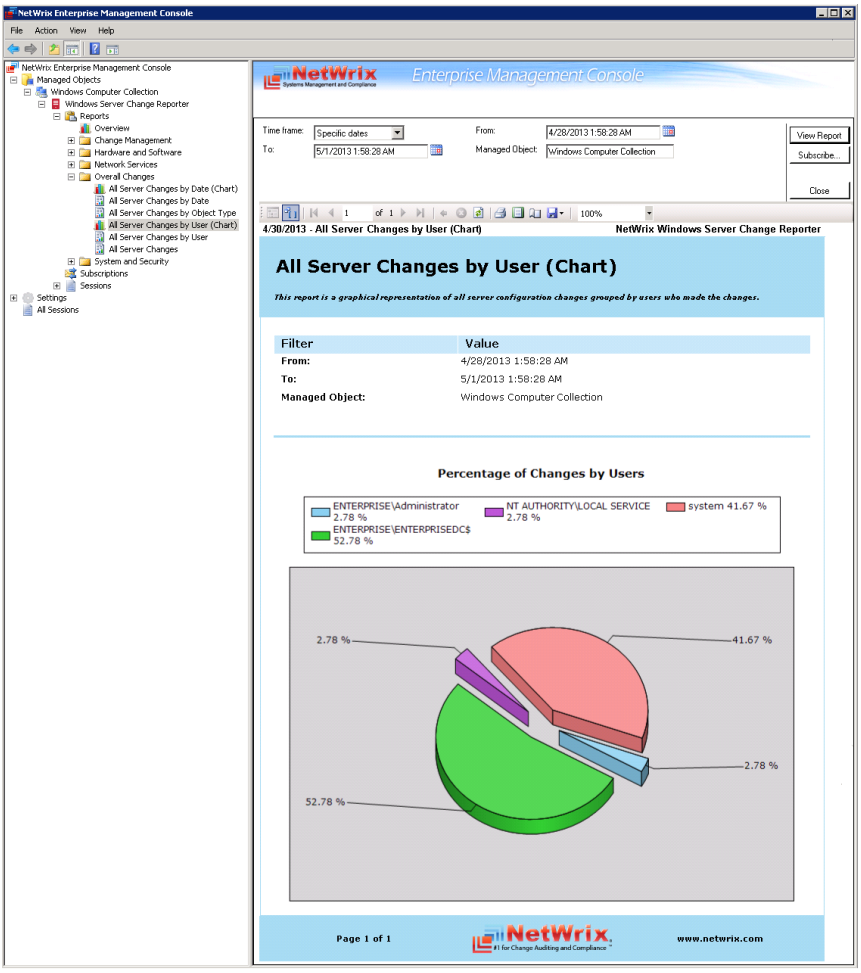


Chart reports provide a visual representation of the changes statistics on the monitored computers:

Figure 36: All Server Changes by User (Console)



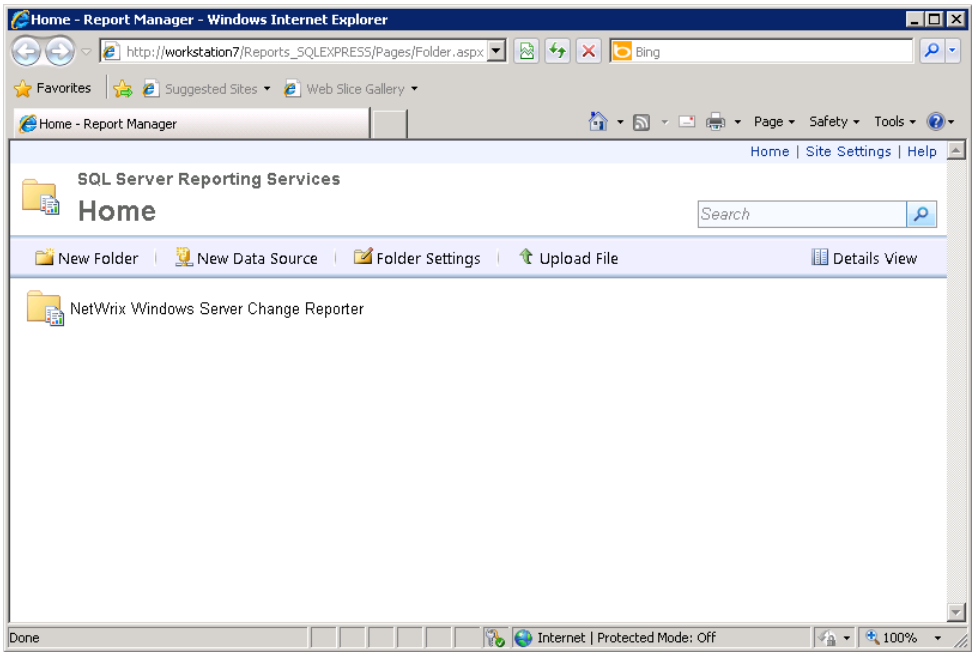
6.3.2. Viewing Reports in Web Browser

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 → 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:

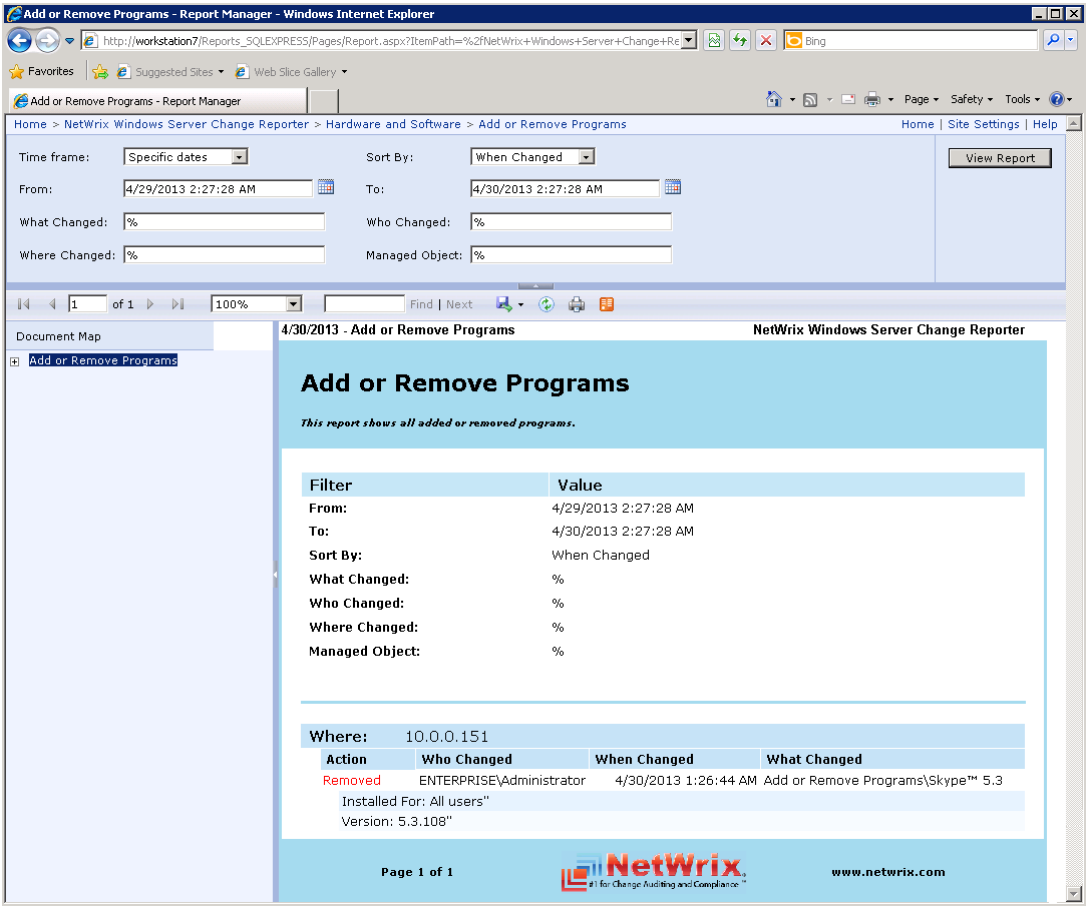
Figure 37: SQL Server Reporting Services Page



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:

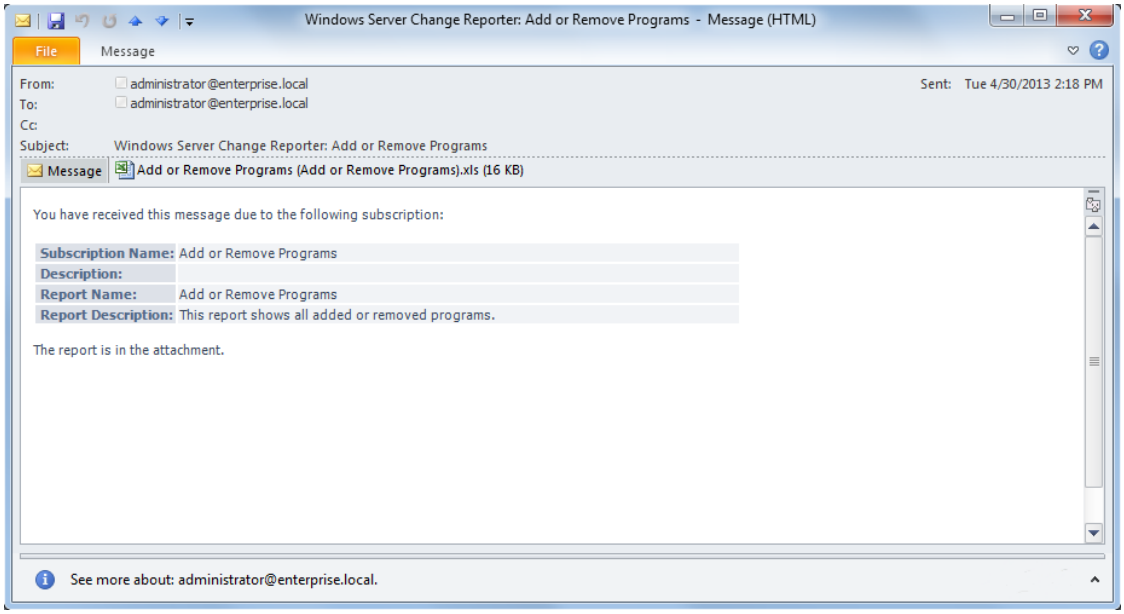
Figure 38: Add or Remove Programs Report (Web Browser)



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:

Figure 39: Report Delivered by Subscription



This section provides detailed instructions on how to:

- Create a Subscription
- Modify a Subscription
- Force on-demand report delivery

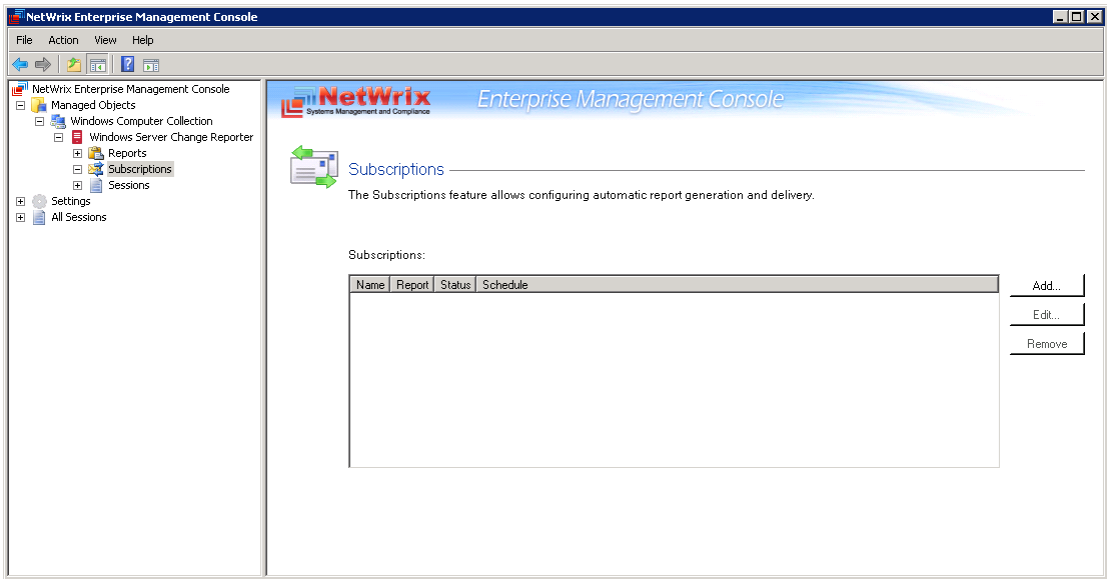
6.4.1. Creating a Subscription

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 6.2.2 Uploading Report Templates to the Report Server.

Procedure 14. To create a Subscription

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

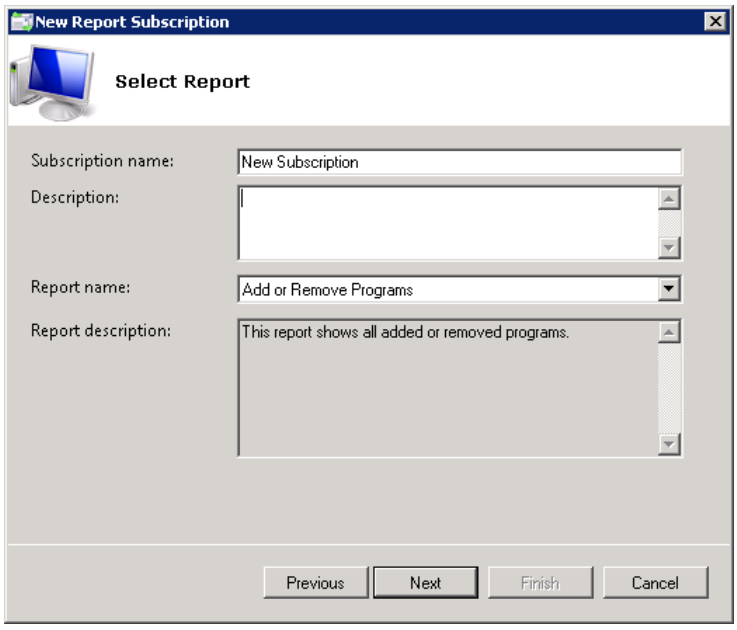
Figure 40: Subscriptions Page



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:

Figure 41: Select Report



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

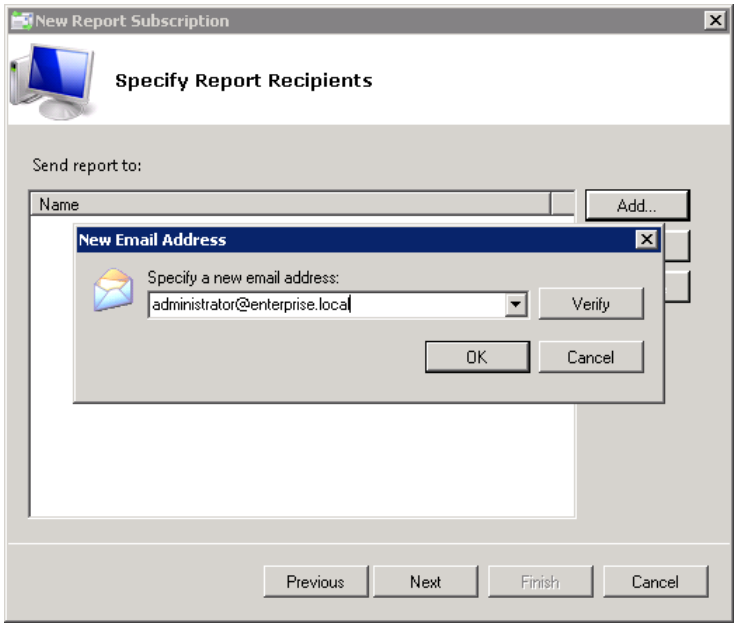
Table 8: Subscription Settings

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.

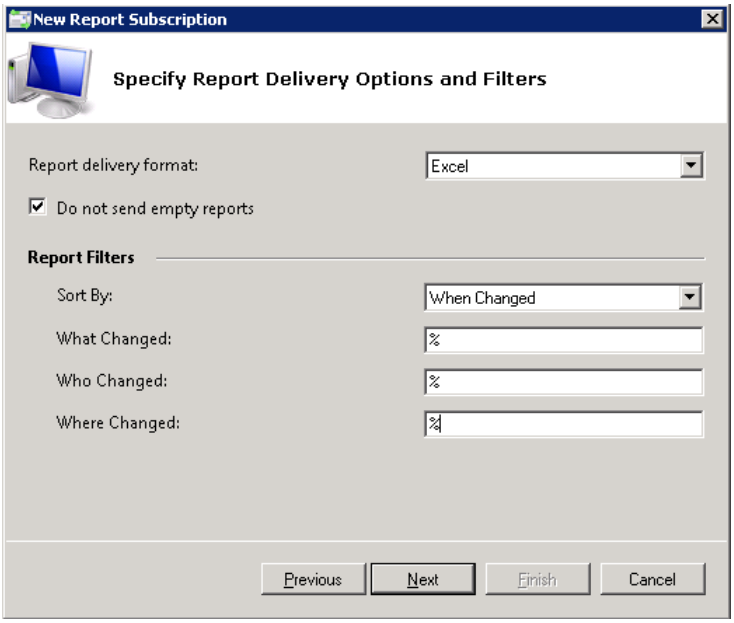
5. On the **Specify Report Recipients** step, click the **Add** button and specify the email address(es) of the report recipient(s). It is recommended to click the **Verify** button. The system will send a test message to the specified address and will inform you if any problems are detected. Click **OK**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

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.

Figure 43: Specify Report Delivery Options and Filters

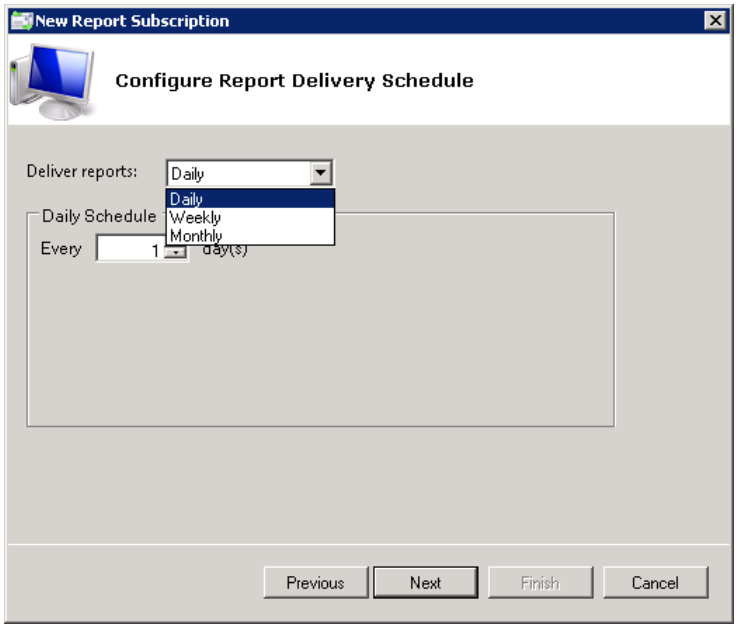


7. On the **Configure Report Delivery Schedule** step, specify the report delivery schedule. The following options are supported:

   - Daily: reports will be delivered at a specified interval (in days) at 3:00 AM.
   - Weekly: reports will be delivered on the specified day(s) of the week at 3:00 AM.
   - Monthly: 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.

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.

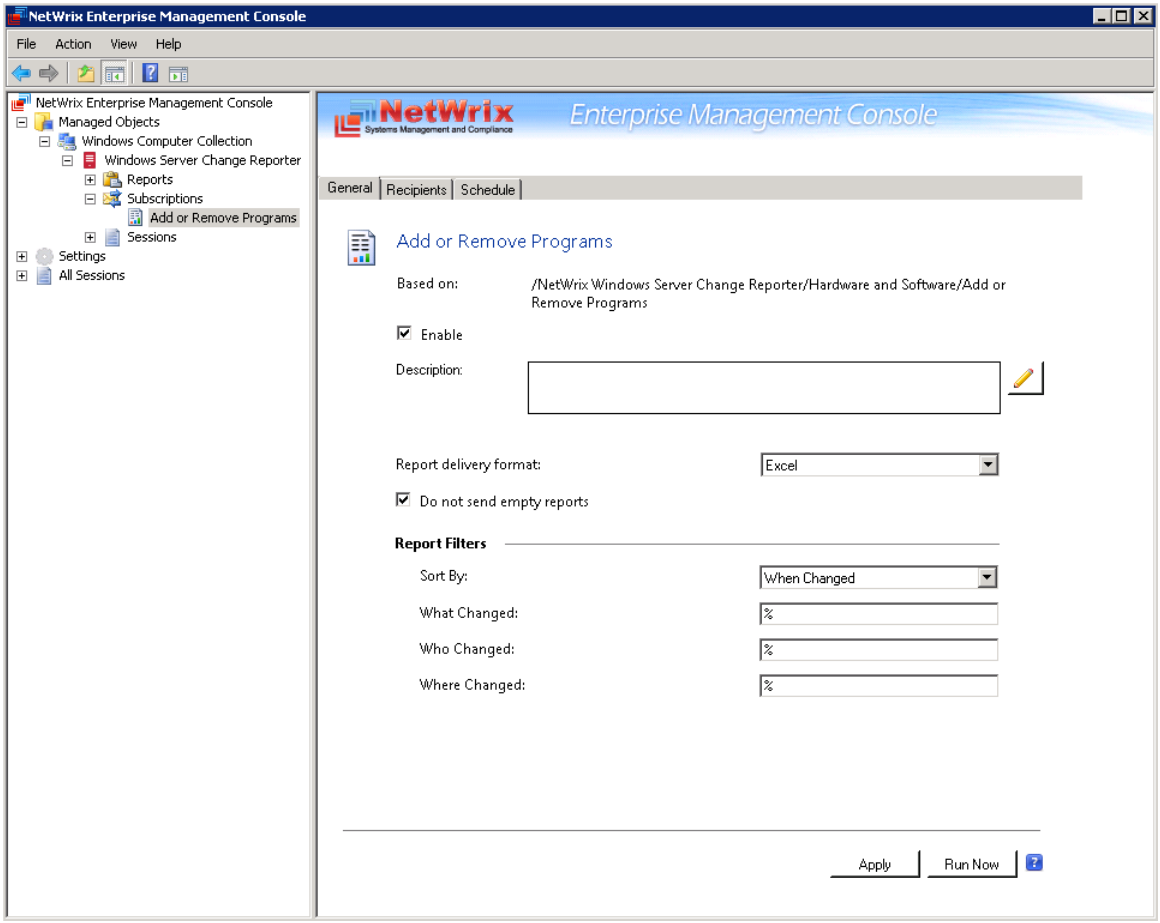
6.4.2. Modifying a Subscription

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

Procedure 15. To modify a Subscription

1. 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:

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

1. 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

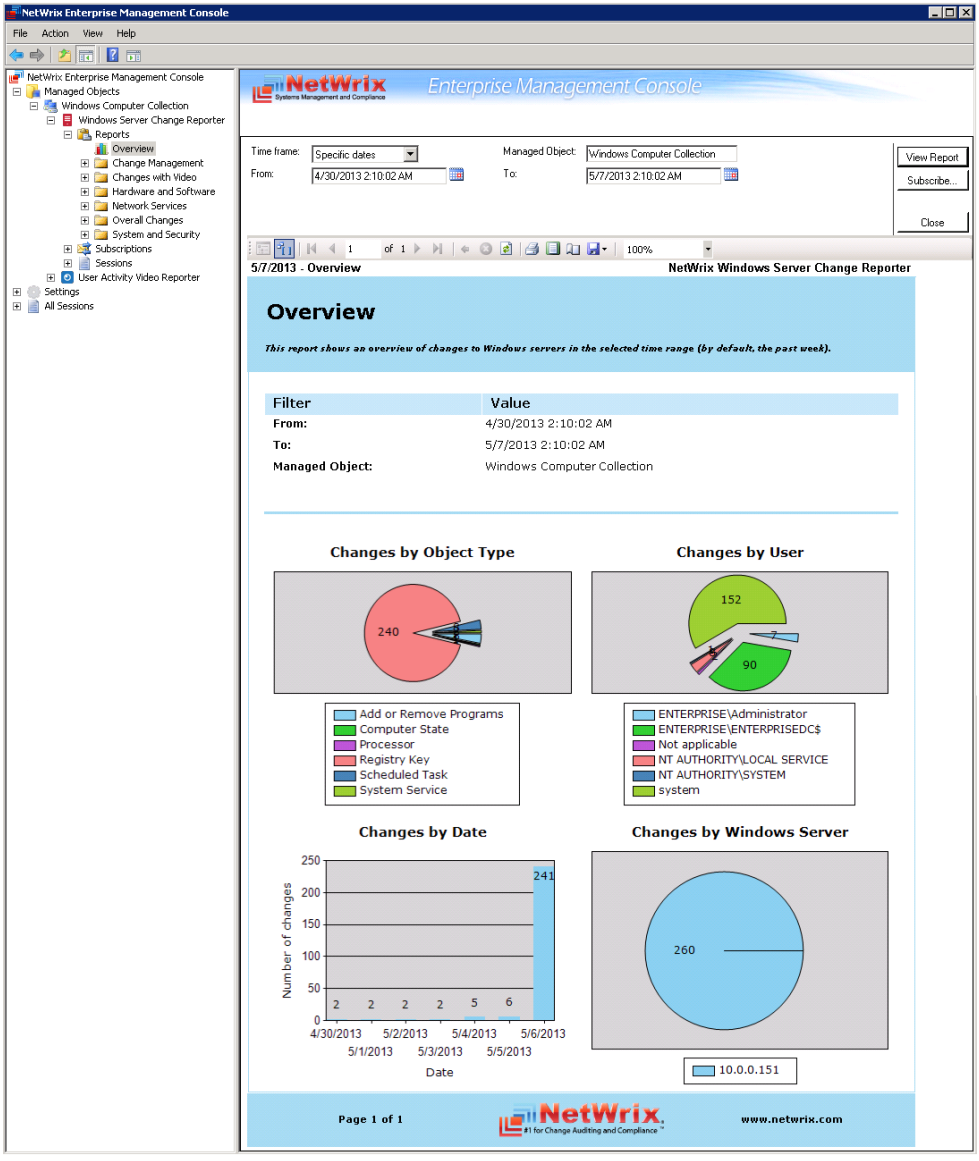
Netwrix Windows Server Change Reporter provides a visual representation of all changes to the monitored computers in the Overview report.

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

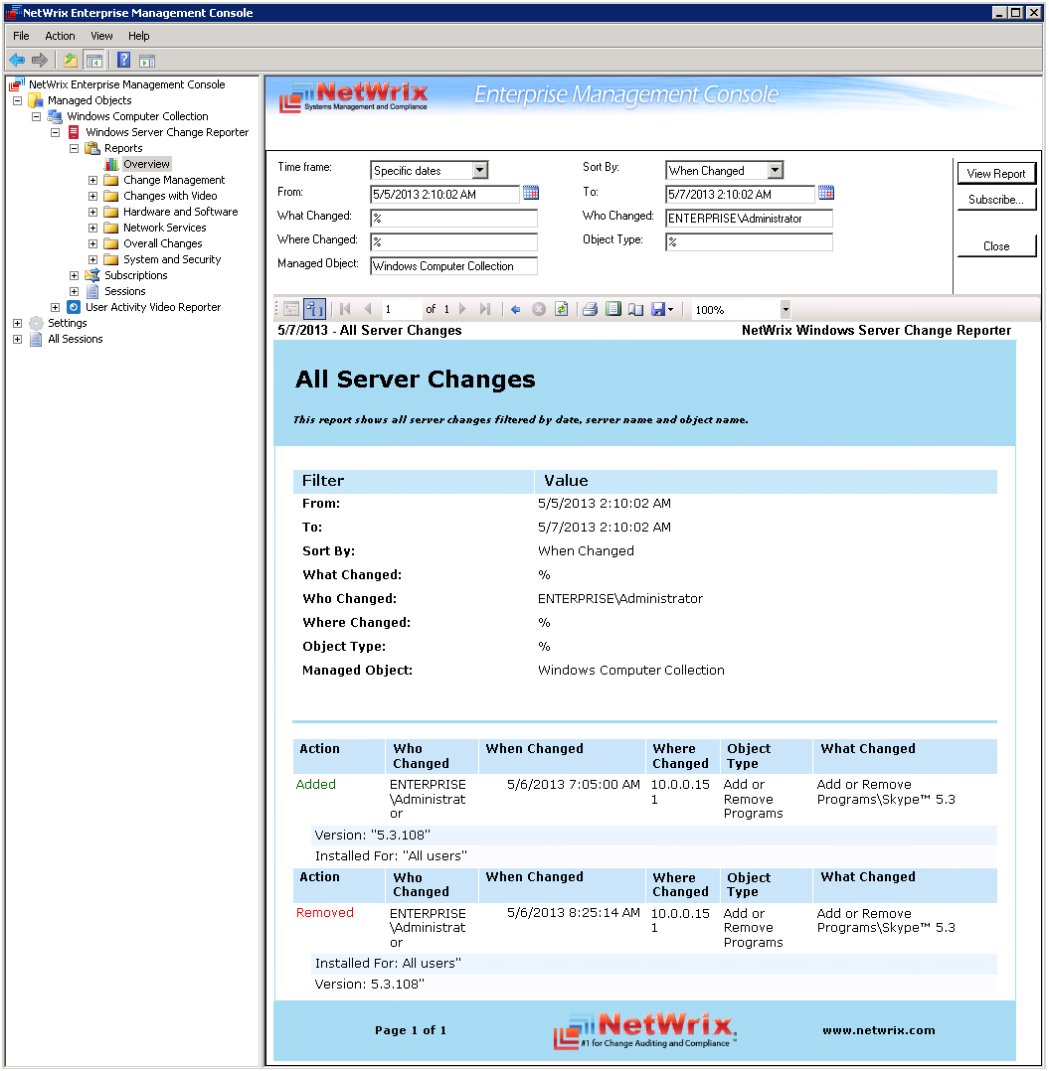
1. In Netwrix Management Console, expand the **Managed Objects** → **<Managed_Object_name>** → **Windows Server Change Reporter** → **Reports** and select the **Overview** report.
2. Specify filters to the report and click the **View Report** button to apply them. The report will be displayed showing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

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.

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*.

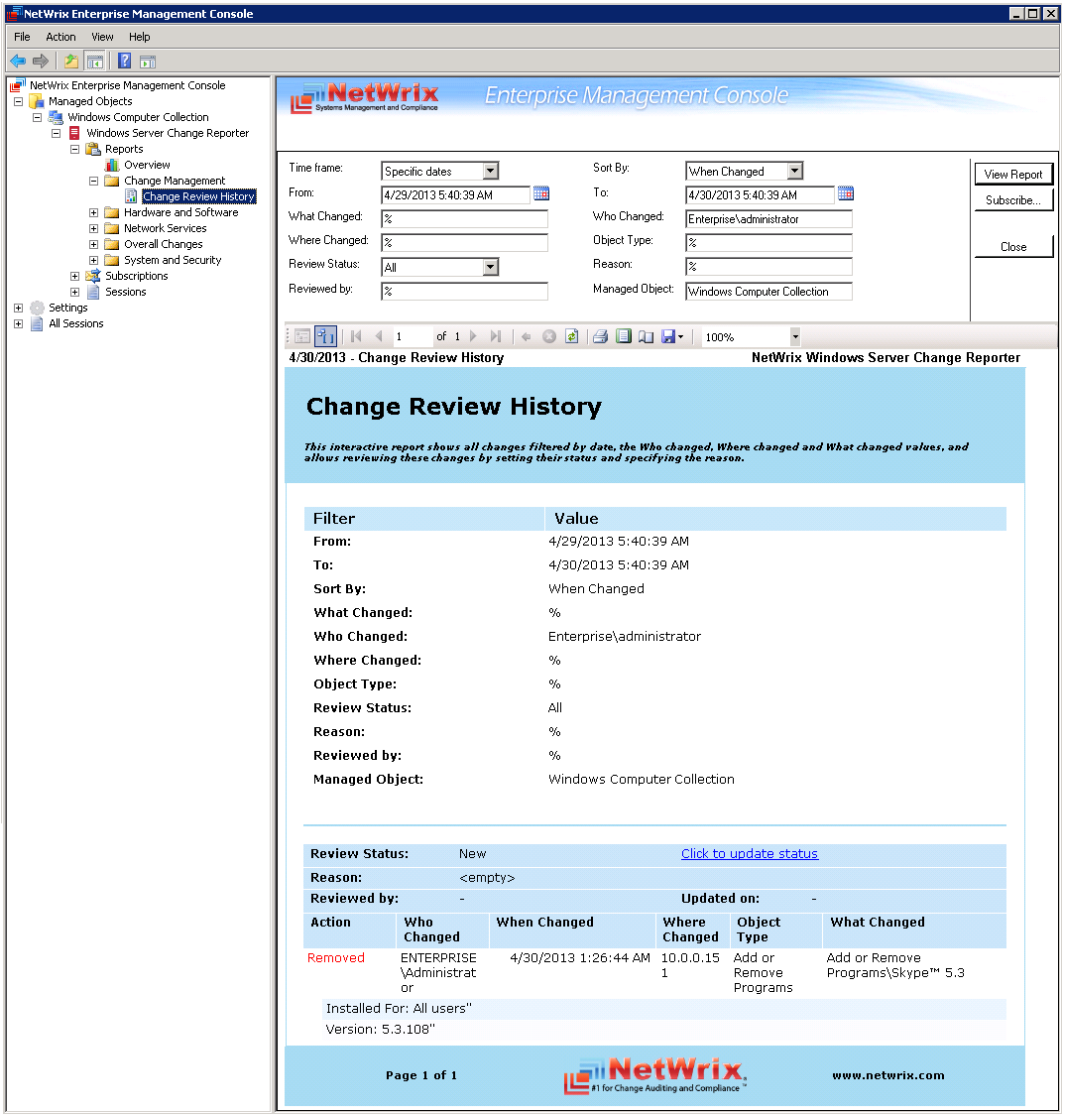
6.6.1. Reviewing Changes to Windows Server Configuration

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

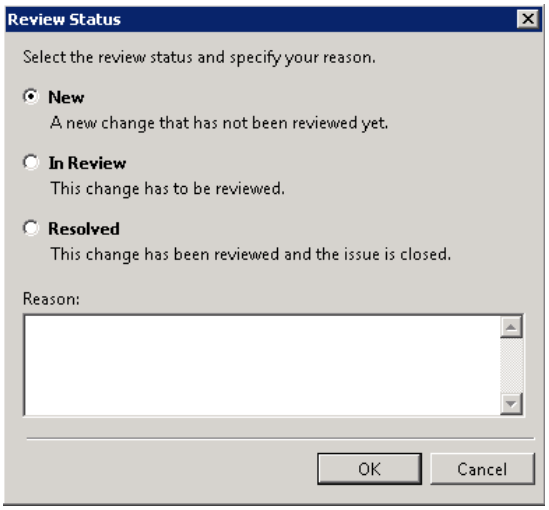
1. In Netwrix Management Console, expand the **Managed Objects → <Managed_Object_name> → Windows Server Change Reporter → Reports → Change Management** node and select the **Change Review History** report.
2. Specify filters to the report and click the **View Report** button to apply them. The report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

Figure 48: Change Review History Report



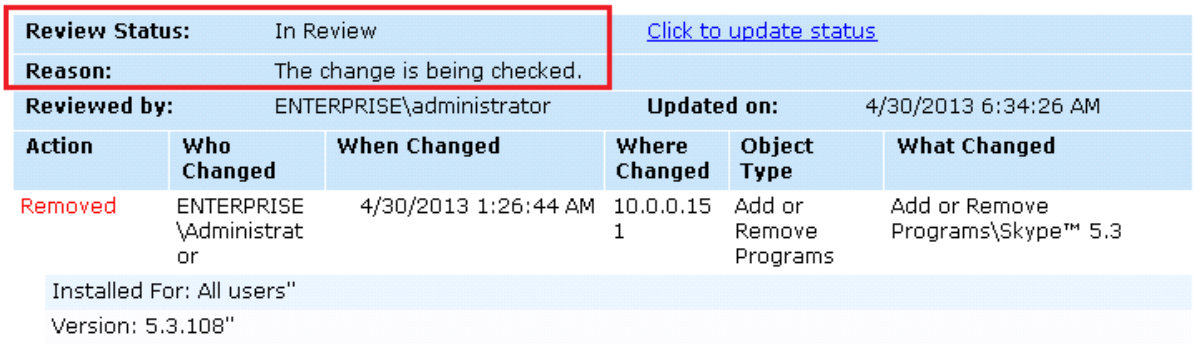
3. Click the **Click to update status** link, select one of the statuses and provide your comments if required.

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

Figure 50: Updated Review Status



Review Status:	In Review		Click to update status		
Reason:	The change is being checked.				
Reviewed by:	ENTERPRISE\administrator		**Updated on:**	4/30/2013 6:34:26 AM	
Action	**Who Changed**	**When Changed**	**Where Changed**	**Object Type**	**What Changed**
Removed	ENTERPRISE\Administrator	4/30/2013 1:26:44 AM	10.0.0.151	Add or Remove Programs	Add or Remove Programs\Skype™ 5.3
Installed For: All users"					
Version: 5.3.108"					

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.

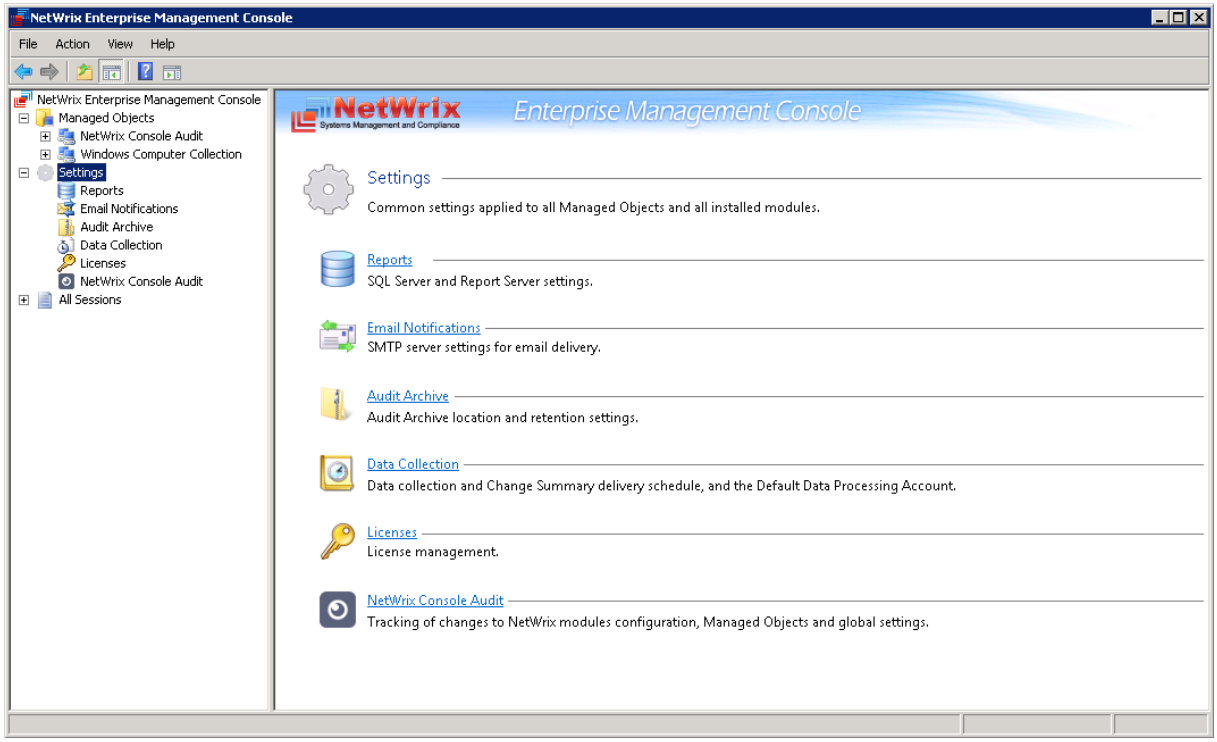
7. CONFIGURING GLOBAL SETTINGS

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 4.2 Modifying Managed Object Settings.

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

Figure 51: Settings Page



The following global settings can be configured:

- Reports settings
- Email Notifications settings
- Audit Archive settings
- Data Collection settings
- Licenses settings
- Netwrix Console Audit

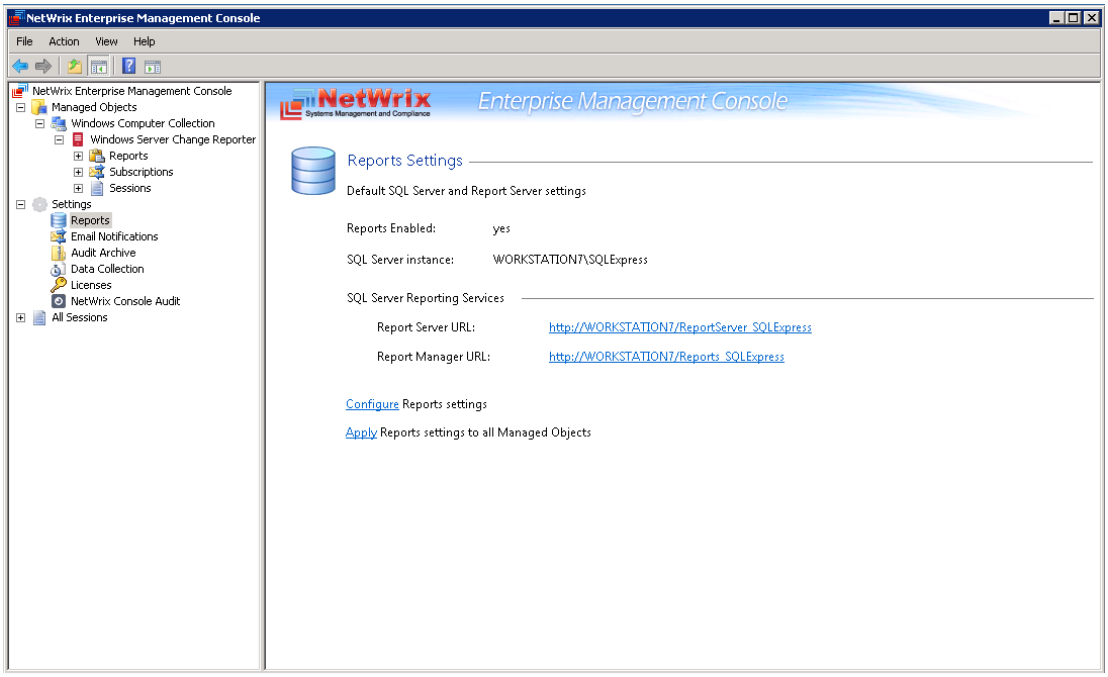
7.1. Configuring the Reports Settings

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

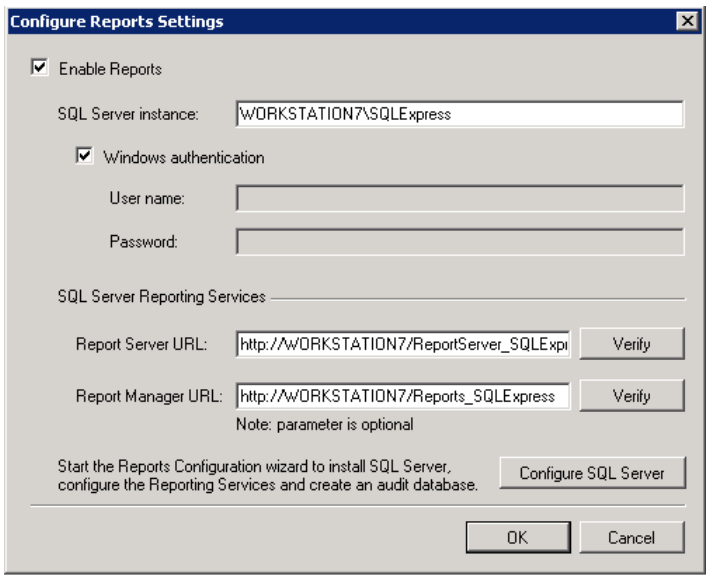
1. In Netwrix Management Console, expand the **Settings** node and select the **Reports** node. Alternatively, you can click **Reports** in the **Settings** page. The following page will be displayed showing the current Reports settings:

Figure 52: Settings: Reports



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

Figure 53: Reports Settings



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 Table 3: Reports Parameters.

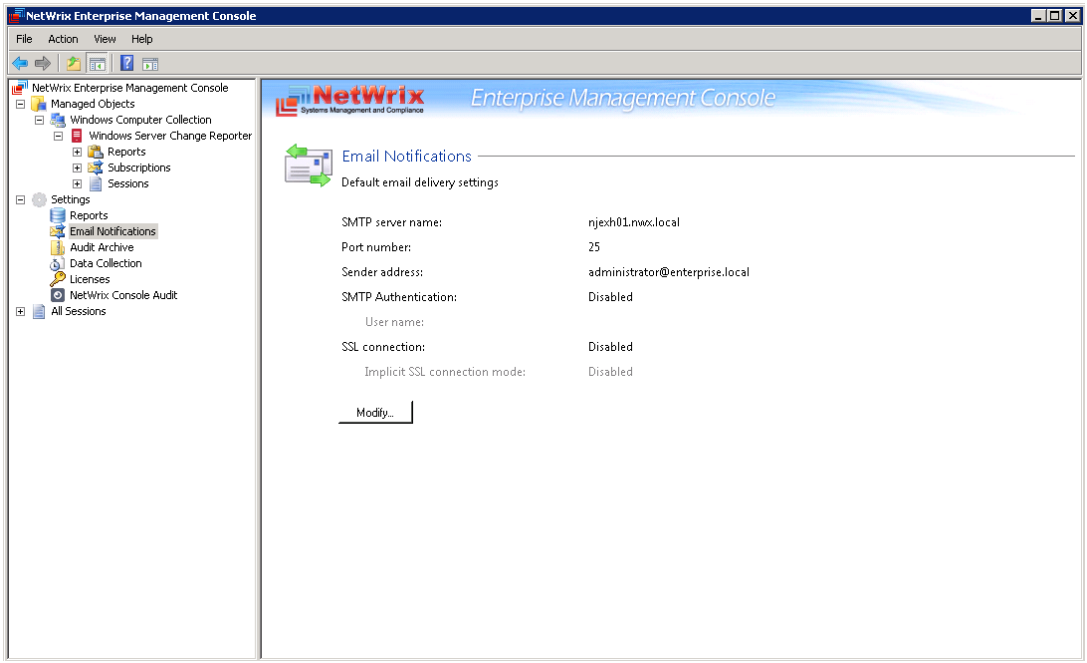
7.2. Configuring the Email Notifications Settings

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

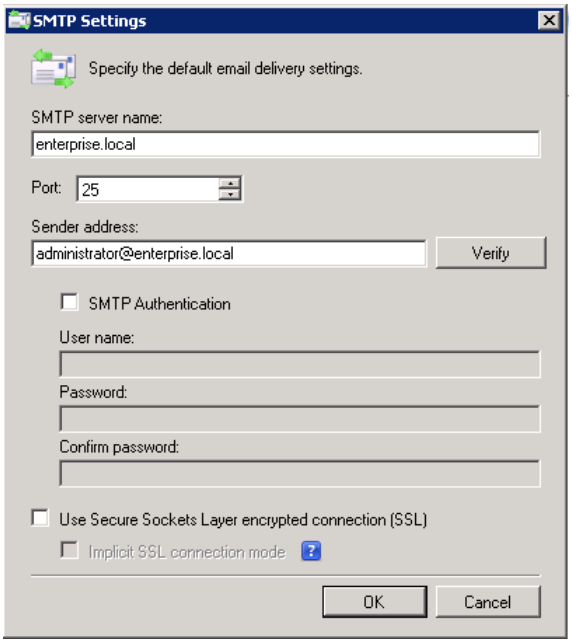
1. In Netwrix Management Console, expand the **Settings** node and select **Email Notifications**. Alternatively, you can click **Email Notifications** in the Settings page. The following page will be displayed showing the current email settings:

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



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

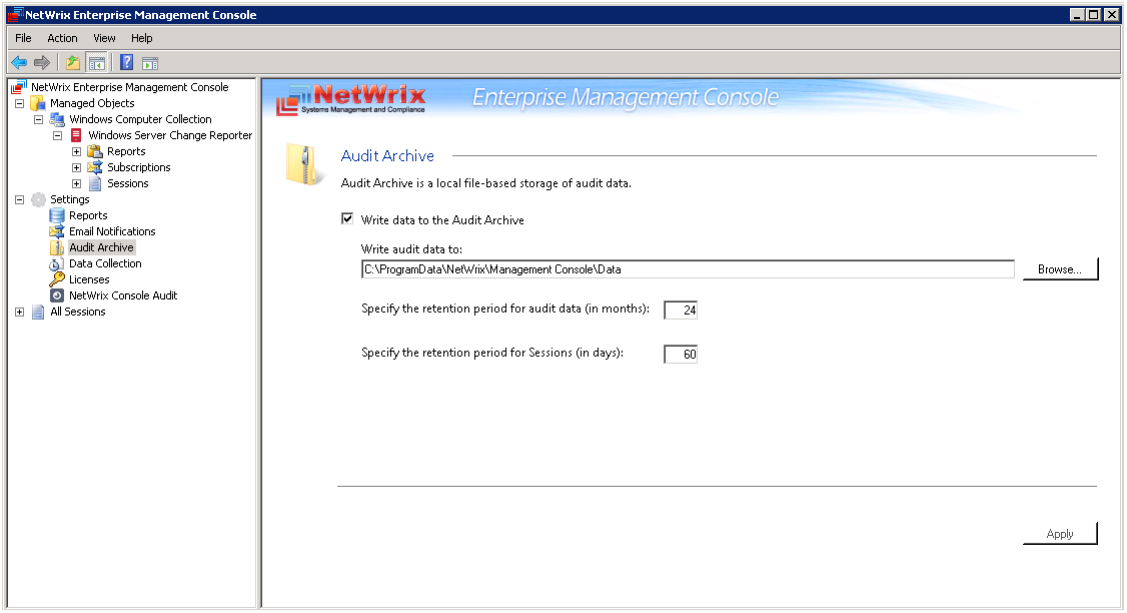
7.3. Configuring Audit Archive Settings

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:

Figure 56: Settings: Audit Archive



2. Modify the following settings if necessary:

Table 9: Audit Archive Settings

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.

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.

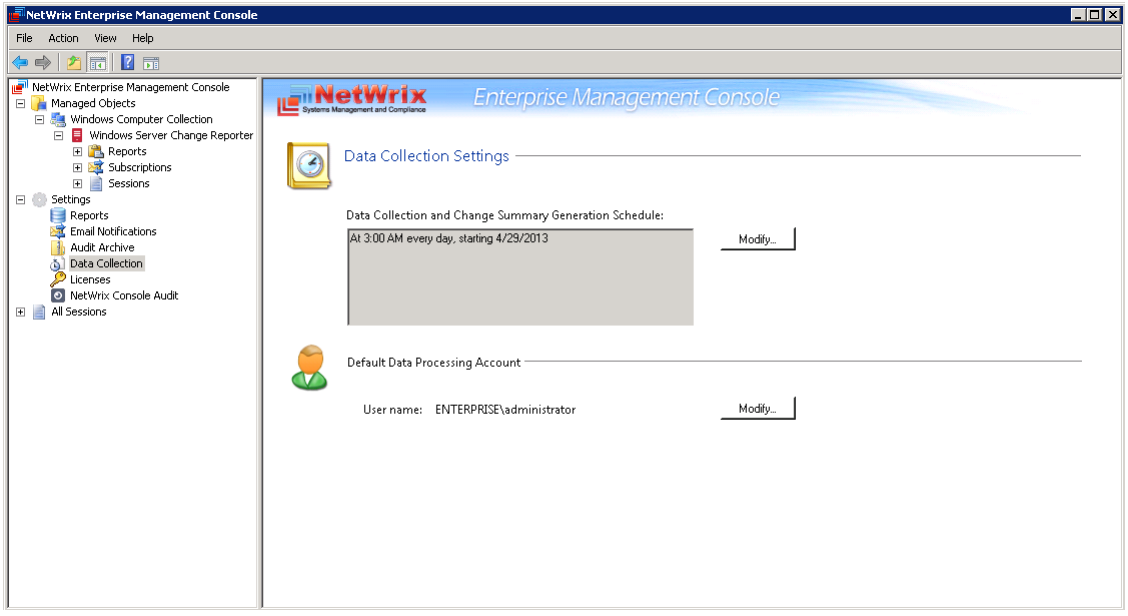
7.4. Configuring Data Collection Settings

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:

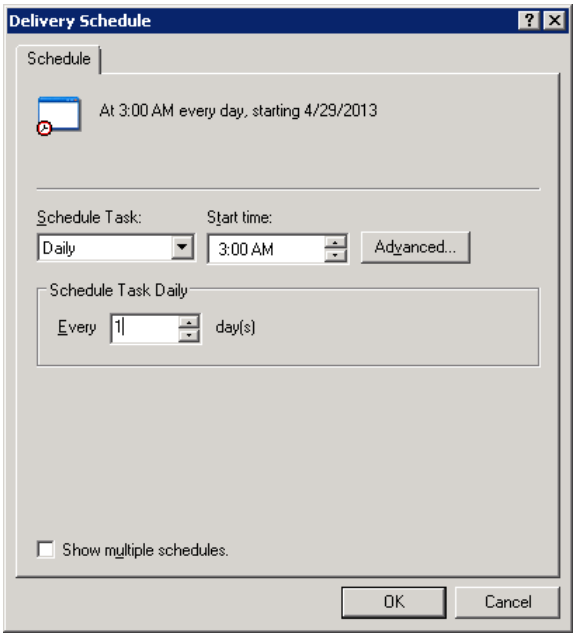
Figure 57: Settings: Data Collection



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

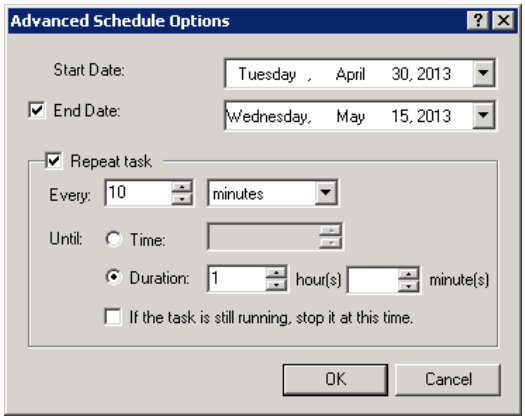
3. In the **Delivery Schedule** dialog, specify a new time and frequency for the data collection:

Figure 58: Delivery Schedule



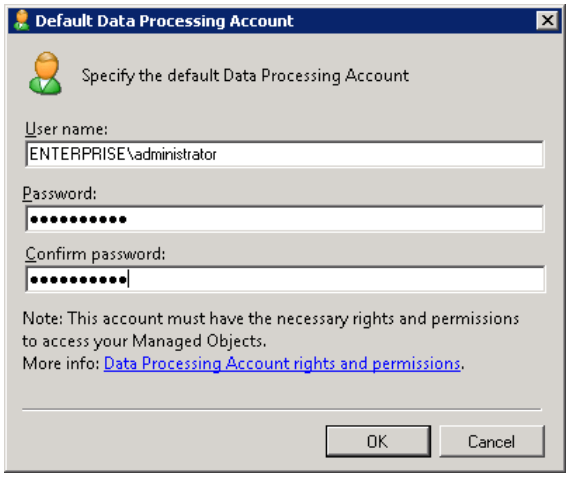
4. To access the advanced schedule options, click the **Advanced** button, and select the required options:

Figure 59: Advanced Schedule Options



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**:

Figure 60: Default Data Processing Account



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 Netwrix Windows Server Change Repoter Installation and Configutation Guide.

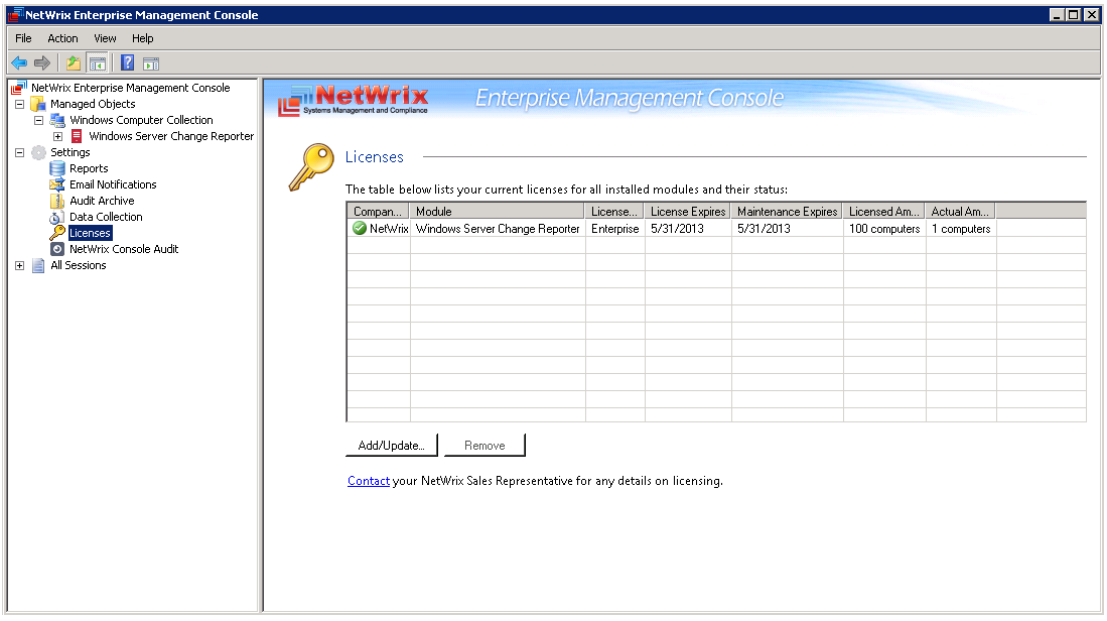
7.5. Configuring License Settings

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:

Figure 61: Settings: Licenses



2. Perform one of the following operations if necessary:

- To add/update your licenses, 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.

- To remove a license, select it from the list and click the **Remove** button. Then click **Yes** in the confirmation dialog.

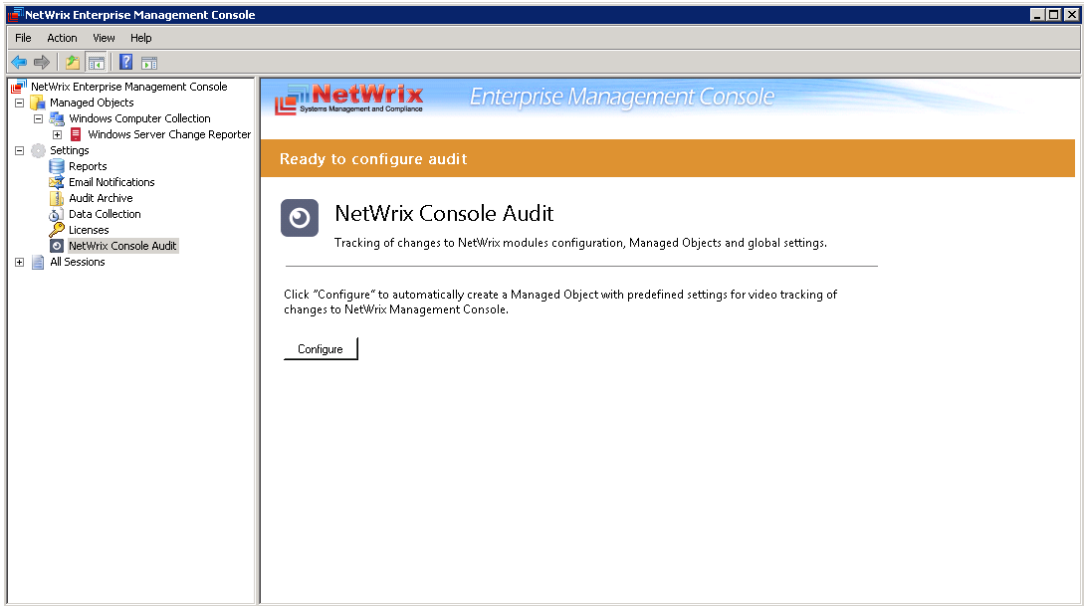
7.6. Configuring Netwrix Console Audit

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:

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:

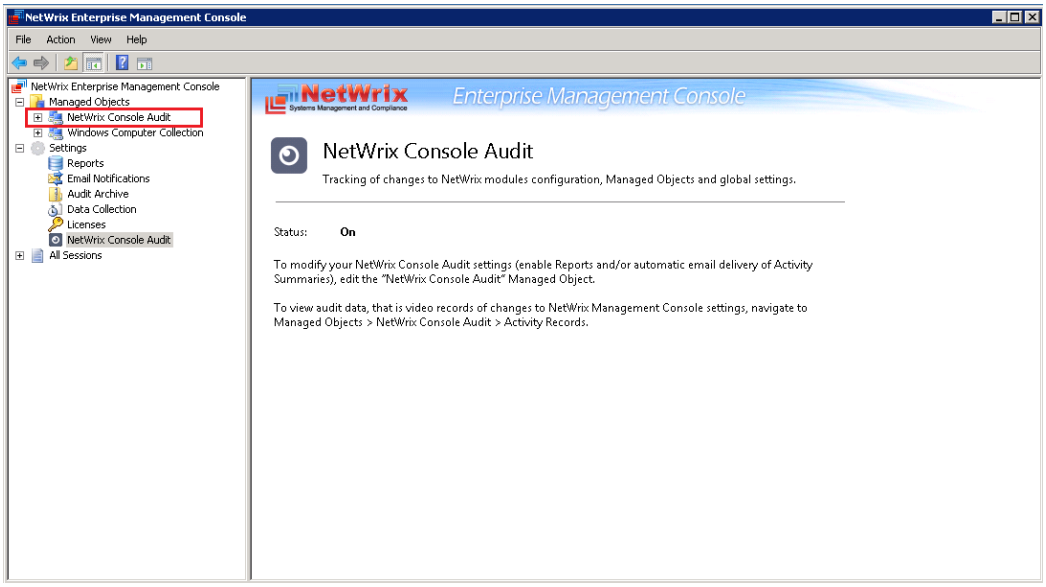
Table 10: Managed Object Default Settings

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

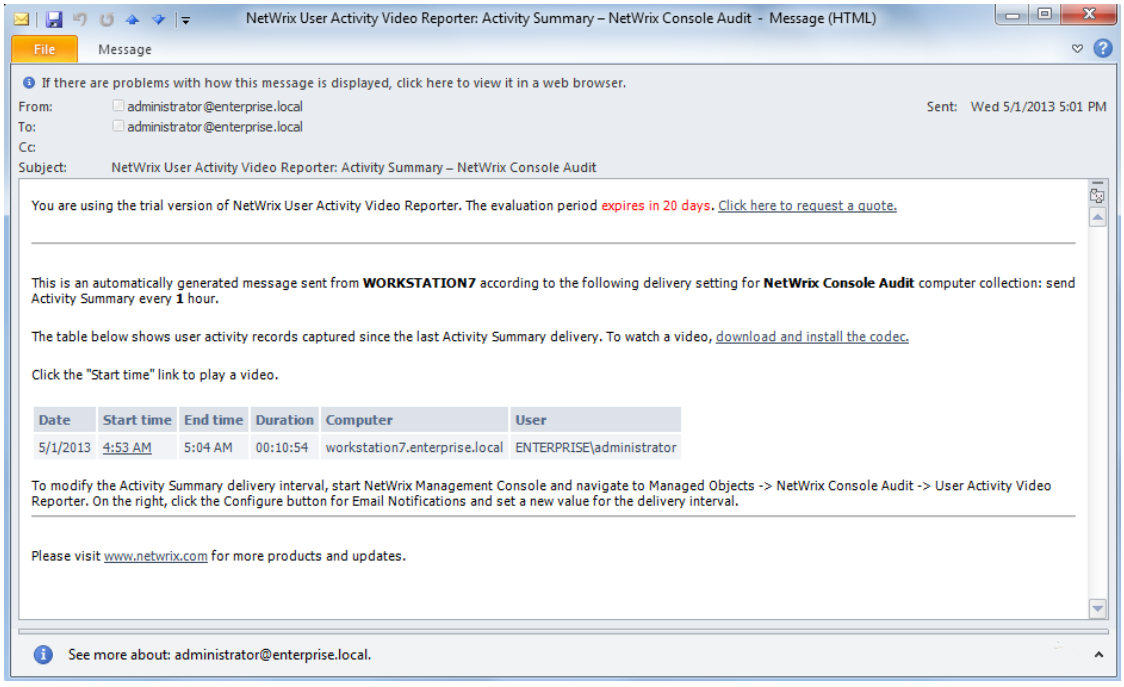
3. Click **OK** when the confirmation message is displayed. The newly created Managed Object will appear under the **Managed Objects** node, and the status of Netwrix Console Audit will change to "On":

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:

Figure 64: Activity Summary



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 → <your Managed_Object_name> → User Activity Video Reporter → 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 NetWrix User Activity Video Reporter Administrator's Guide.

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.

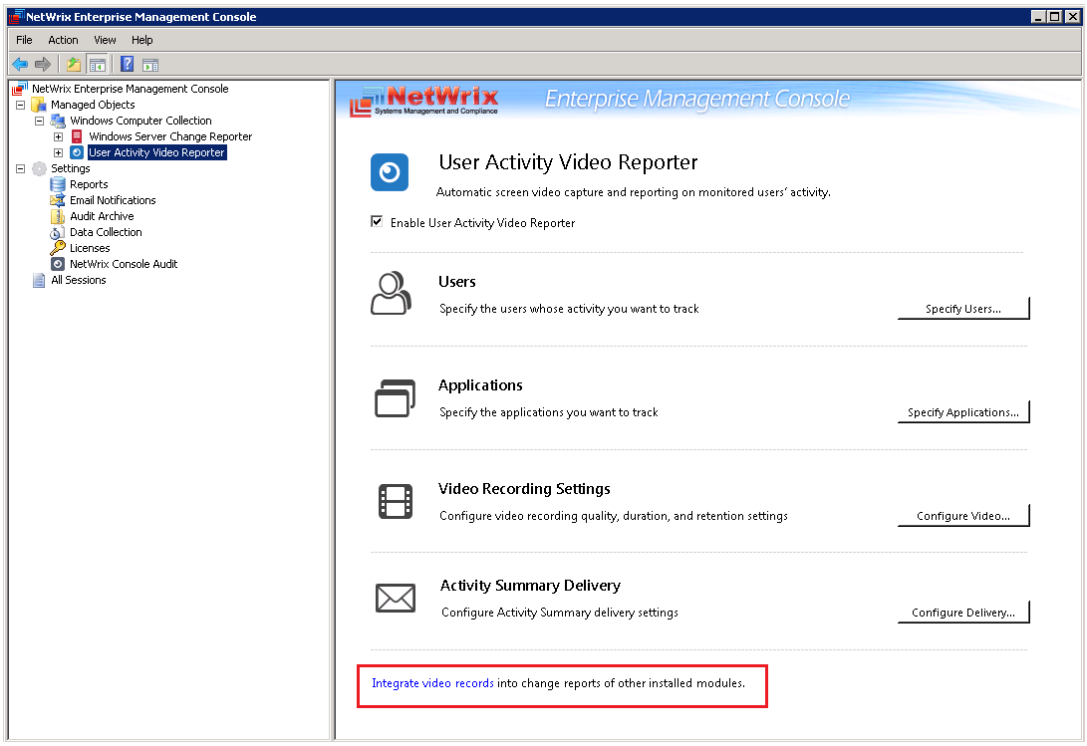
Integration can be enabled if the following conditions are met:

- 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 Netwrix User Activity Video Reporter Administrator's Guide.
- 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 5.2.1 Generating Change Summary on Demand.

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

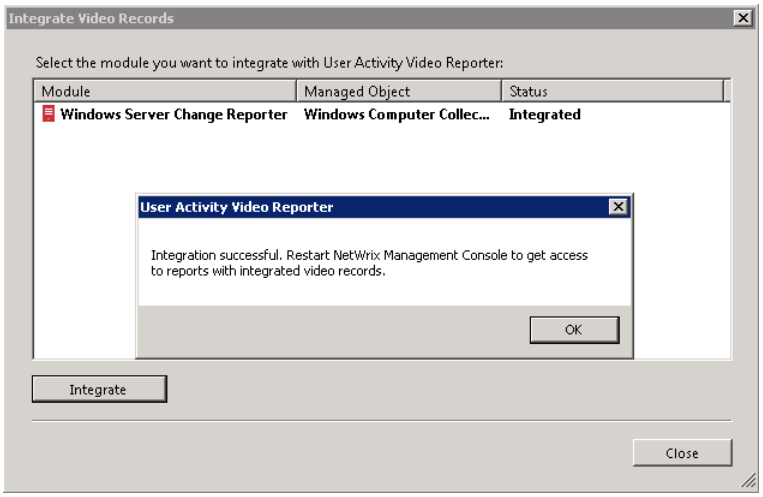
1. In the Netwrix Management Console tree, navigate to **Managed Objects → <Managed_Object_name> → User Activity Video Reporter**.
2. Click the **Integrate video records** link at the bottom of the **User Activity Video Reporter** main page:

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

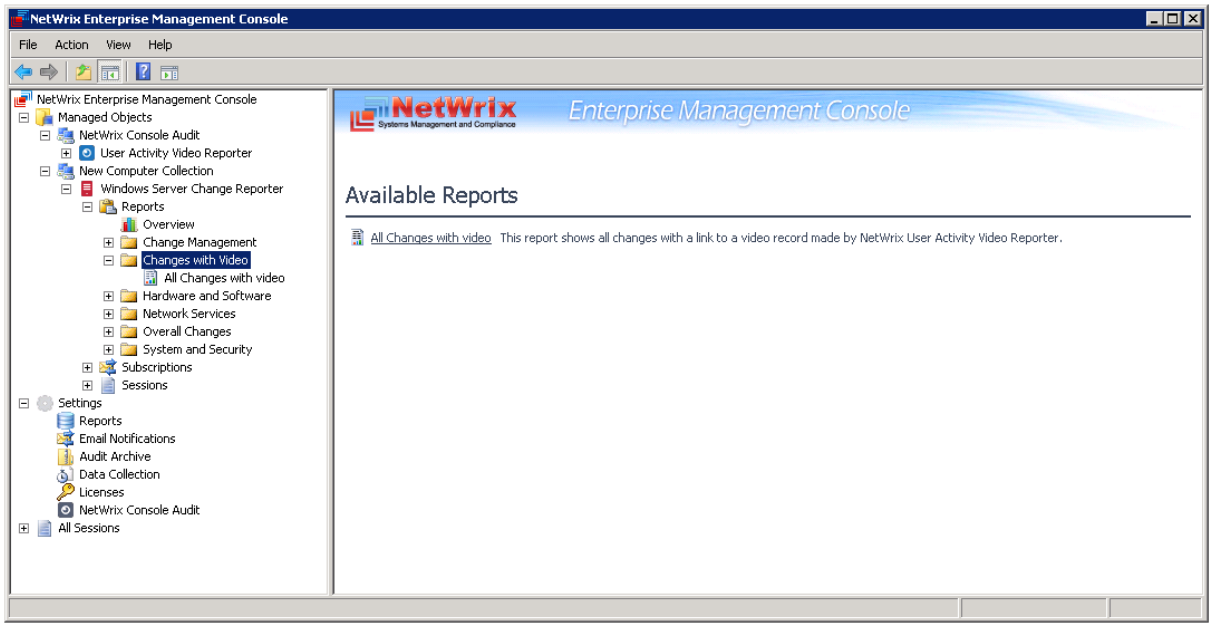


4. If the operation is completed successfully, the status of the selected module changes to "Integrated". If it fails, a message is displayed explaining the reason why integration has failed.

5. Restart Netwrix Management Console for the changes to take effect.

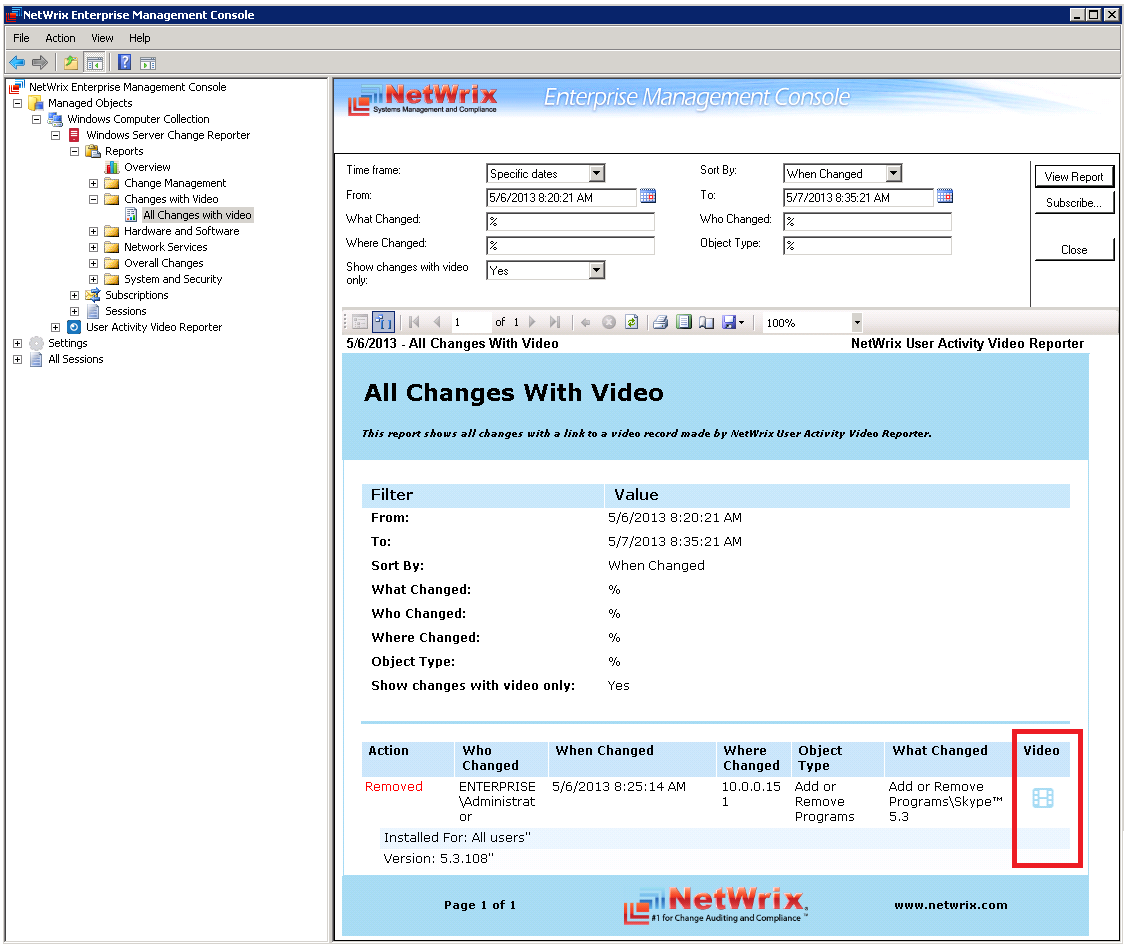
The report with videos on the changes made to your target computers is available in the **Changes with Video** folder under the **Reports** node of the relevant Managed Object:

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:

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.

Table 11: Netwrix Windows Server Change Reporter Configuration Files

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.

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

Table 12: Monitored Objects: Computer Settings

Object Type	Attributes
Computer Name	• Computer Description • Name • Domain
Environment Variables	• Type • Value
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

A.2 Add/Remove Programs

Table 13: Monitored Objects: Software Installation

Object Type	Attributes
Add or Remove Programs	• Installed For* • Version

A.3 Services

Table 14: Monitored Objects: Services

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

A.4 Hardware

Table 15: Monitored Objects: Hardware and System Drivers

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
Infrared*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
Keyboard*	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code

	• Layout • Name • Status
Logical Disk*	• Description • File System • Size (bytes) • Status
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 • DHCP Server • 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
Parallel Ports*	• Configuration 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) • Status • Manufacturer • 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: Monitored Objects: Scheduled Tasks

Object Type	Attributes
Scheduled Task	• Account Name • Application • Comment • Creator • Enabled • Parameters • Triggers

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*

Table 18: Monitored Objects: 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

	• 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 • FQDN for target domain • Owner name • TTL
DNS DNSKEY	• Algorithm • Container name • Key type • Key (base 64) • Name type • Owner name • Protocol • Signatory field • TTL
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

	• TTL
DNS MG	• Container name • Member mailbox • Owner name • TTL
DNS MINFO	• Container name • Error mailbox • Owner name • Responsible mailbox • TTL
DNS MR	• Container name • Owner name • Replacement mailbox • TTL
DNS MX	• Container name • FQDN of mail server • Mail server priority • Owner name • TTL
DNS NAPTR	• Container name • Flag string • Order • Owner name • Preference • Regular expression string • Replacement domain • Service string • TTL
DNS NS	• Container name • Name servers • Owner name • TTL
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

Table 20: Monitored Objects: 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|)

	\\Microsoft\\MSDTC(|\\.*) • 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:

Table 21: Product Documentation

Document Name	Overview
Netwrix Windows Server Change Reporter Administrator's Guide	The current document.
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.
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.
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.