NETWRIX ACTIVE DIRECTORY CHANGE REPORTER

ADMINISTRATOR'S GUIDE

Product Version: 7.2

January 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 Active Directory 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 AD domain for monitoring, refer to NetWrix Active Directory 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 Active Directory Change Reporter functionality, lists its main features and benefits, and explains the product workflow. It also contains information on the product editions and a side-by-side comparison of their features.
- Chapter 3 NetWrix Enterprise Management Console Overview provides a description of NetWrix Enterprise Management Console, which is an integrated interface for most NetWrix products.
- Chapter 4 Managed Object explains how to configure a Managed Object, i.e. an Active Directory domain that you want to monitor for changes. It also explains how to modify Managed Object settings.
- Chapter 5 Data Collection explains the NetWrix Active Directory 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 (including Snapshot Reporting), 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 Real-Time Alerts provides an overview of the Real-Time Alerts feature, and explains how to configure alerts in NetWrix Active Directory Change Reporter. It also contains a detailed algorithm for selecting a correct attribute to define alert filters.
- Chapter 8 Active Directory Object Restore explains how to revert unwanted changes to AD objects using the Active Directory Object Restore wizard integrated with NetWrix Active Directory Change Reporter.
- Chapter 9 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 10 Additional Configuration provides a description of the product additional configuration options, such as enabling monitoring of the Configuration and Schema partitions, enabling integration with SIEM solutions and excluding data types from data collection and product reports.

- A Appendix: Monitored Object Types and Attributes provides links to a list of all Active Directory object classes and attributes monitored by NetWrix Active Directory Change Reporter.
- B Appendix: SQL Database Retention Script contains a SQL script used to configure the SQL database retention policy.
- C Appendix: NetWrix Active Directory Change Reporter Registry Keys contains a description of the product registry keys that can be used for additional configuration.
- D Appendix: Related Documentation contains a list of all documents published to support NetWrix Active Directory Change Reporter.

2. PRODUCT OVERVIEW

Microsoft Active Directory change auditing has become a mission-critical activity in business networks. Unauthorized changes and errors in Active Directory configuration can put your organization at risk introducing security breaches and compliance issues. Native Active Directory auditing is often inadequate when it comes to supporting such business needs as troubleshooting, security auditing, change monitoring, and reporting, many of which are driven by the necessity for organizations to comply with external industry and legislative requirements.

NetWrix Active Directory Change Reporter fills this functional gap by tracking all additions, deletions, and modifications made to Active Directory users, groups, computers, OUs, group memberships, permissions, domain trusts, AD sites, FSMO roles, AD schema, Group Policy and Exchange objects, settings and permissions.

The product collects data on changes made to the monitored Active Directory domain and generates audit reports showing the before and after values for WHO changed WHAT, WHEN and WHERE in a human-readable format without the overhead of resolving complicated native identifiers.

NetWrix offers long-term data archiving that uses a two-tiered system:

- Audit Archive, a local file-based storage
- SQL Server database

NetWrix offers both agent-based and agentless data collection methods. The use of agents is recommended for distributed deployments or multi-site networks due to their ability to compress network traffic.

NetWrix Active Directory Change Reporter employs AuditAssurance™, a patent-pending technology that does not have the disadvantages of native auditing or SIEM (security Information and Event Management) solutions that rely on a single source of audit data. The AuditAssurance™ technology consolidates audit data from multiple independent sources (event logs, configuration snapshots, change history records, etc.), and, therefore, can detect a change even if one or several sources of information do not contain all of the required data (e.g. because it was deleted, overwritten, etc.). The AuditAssurance™ technology always ensures you get a complete and concise picture of what changes take place in your monitored environment.

NetWrix Active Directory Change Reporter can be purchased separately, but it is also available as part of a larger change reporter pack which automates auditing of the entire Active Directory infrastructure. The NetWrix Active Directory Change Reporter installation pack consists of the following modules:

- NetWrix Active Directory Change Reporter
- NetWrix Group Policy Change Reporter
- NetWrix Exchange Change Reporter

Note: This guide only covers the configuration and usage of the NetWrix Active Directory Change Reporter module. For information on other modules, refer to NetWrix Group Policy Change Reporter Administrator's Guide and NetWrix Exchange Change Reporter Administrator's Guide respectively.

2.1. Key Features and Benefits

NetWrix Active Directory Change Reporter is a tool for automated auditing and reporting on changes to the monitored Active Directory environment. It allows you to do the following:

- **Monitor day-to-day administrative activities**: the product captures detailed information on all changes made to the monitored Active Directory environment, including the information on WHO changed WHAT, WHEN and WHERE. Audit reports and real-time email notifications facilitate review of daily activities.
- **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.
- **Streamline change control**: the integrated Active Directory Object Restore tool streamlines the restore of any undesired or potentially harmful changes to your Active Directory environment.
- **Integrate with SIEM systems**: the product can be integrated with multiple SIEM systems, including RSA enVision®, ArcSight® Logger™, Novell® Sentinel™, NetIQ® Security Manager™, IBM Tivoli® Security Information and Event Manager™ and more. The product can also be configured to feed data to Microsoft System Center Operations Manager, thus providing organizations that use SCOM with fully automated Active Directory auditing and helping protect these investments.

The main NetWrix Active Directory Change Reporter features are:

- **Reports** with the previous and current values for every object- and attribute-level change. Reports are based on SQL Server Reporting Services (SSRS) with over 70 predefined report templates and support for custom reports.
- **Real-time alerts**: email notifications triggered by certain events and sent immediately after they have been detected.
- **Report subscriptions** allow for scheduled report generation and delivery to the specified recipients. You can apply different report filters and select report output format.
- **Snapshot reports**: reports on the current or historical configuration state of your Active Directory environment.
- **Rollback of changes**: the product supports rollback of unwanted changes, down to individual attribute-level changes.
- **Long-term data storage**: allows for recreating the full audit trail of changes made to the monitored Active Directory environment and provides historical reporting for any specified period of time. Organizations can analyze any policy violations which occurred in the past, and maintain ongoing compliance with internal and external regulations.
- **Group Policy and Exchange change auditing**: the Group Policy and Exchange auditing features allow tracking all changes to Group Policy Objects, security policy violations, changes to permissions and more. These are realized through the NetWrix Group Policy Change Reporter module and the NetWrix Exchange Change Reporter module respectively.

2.2. Product Workflow

A typical NetWrix Active Directory 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 Active Directory Change Reporter monitors AD domains and collects audit data on changes and AD configuration snapshots. Audit data is written to a local file-based storage, referred to as the Audit Archive.

3. If an event is detected that triggers an alert, an email notification is sent immediately to the specified recipients.
4. The product emails Change Summaries to the specified recipients daily at 3:00 AM by default.
5. If the Reports functionality is enabled and configured, data is imported from the Audit Archive to a dedicated SQL database. Reports based on audit data can be viewed via NetWrix Enterprise Management Console or in a web browser.

2.3. Product Editions

NetWrix Active Directory 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.

Note: Licenses for different modules of the NetWrix Active Directory Change Reporter pack (i.e. NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter) have to be purchased separately.

Table 1: below outlines the differences between the NetWrix Active Directory Change Reporter editions:

Table 1: NetWrix Active Directory Change Reporter Editions

Feature	Freeware Edition	Enterprise Edition
WHO, WHEN and WHERE fields for every change	No	Yes
The before and after values for every change	No	Yes
SSRS-based Reports, with filtering, grouping and sorting, and dozens of predefined report templates	No	Yes
Custom reports	No	Yes Create manually or order from NetWrix
Predefined reports for SOX, HIPAA, GLBA, and FISMA compliance	No	Yes
Real-Time Alerts	No	Yes
Report Subscriptions	No	Yes
AD Snapshot Reports	No	Yes
Integration with Microsoft System Center Operations Manager Pack (SCOM) (via NetWrix SCOM Management Pack for Active Directory Change Reporter)	No	Yes
Long-term archiving of audit data	No Data is only stored for 4 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 Enterprise Management Console Overview

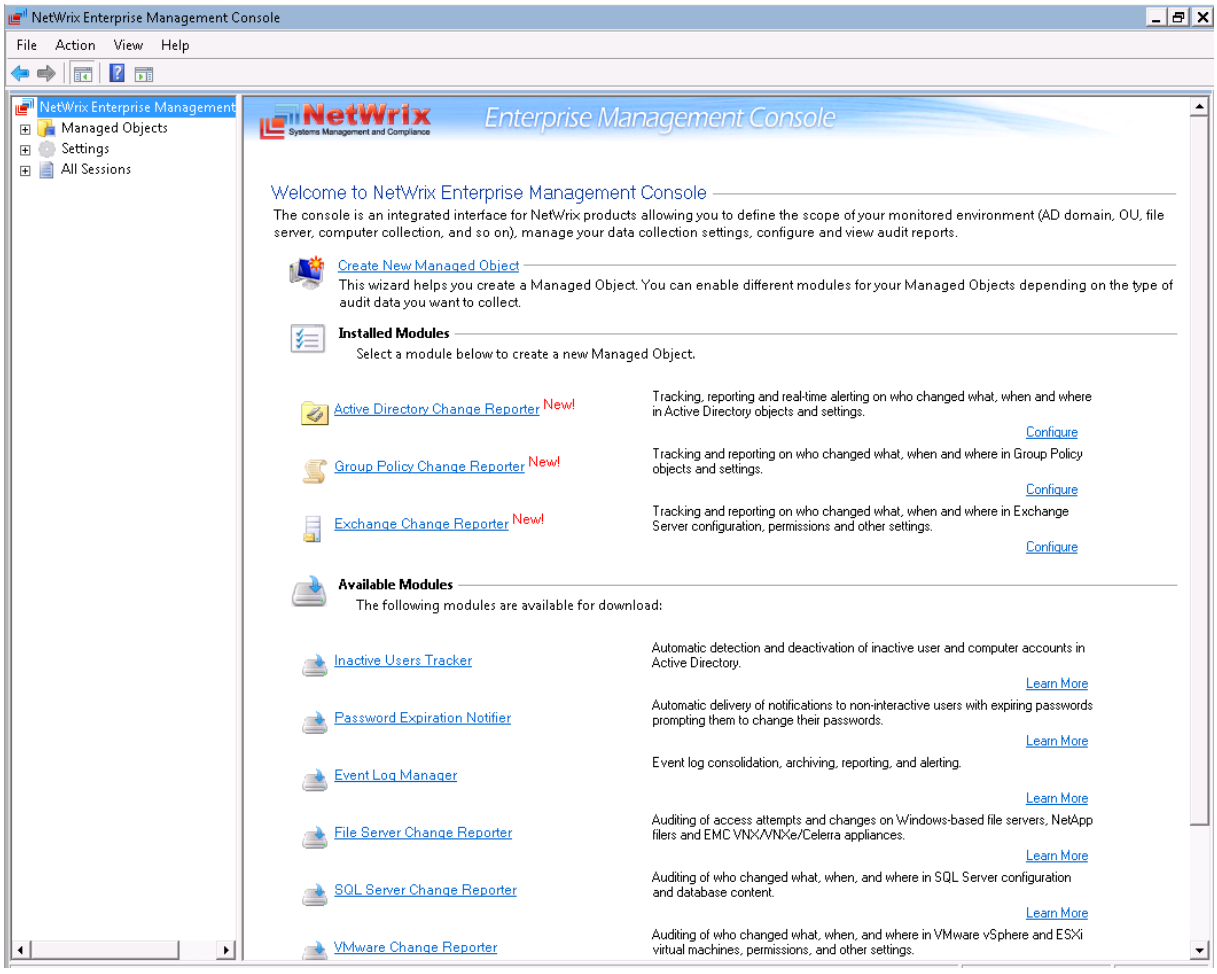
NetWrix Active Directory Change Reporter Enterprise Edition is integrated into NetWrix Enterprise Management Console, an MMC snap-in that allows configuring Managed Objects and their settings, and the reporting options.

NetWrix Enterprise 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 Enterprise Management Console, navigate to **Start → All Programs → NetWrix → Active Directory Change Reporter** and click **Active Directory Change Reporter (Enterprise Edition)**. The console window will be displayed:

Figure 1: NetWrix Enterprise Management Console



4. MANAGED OBJECT

In NetWrix Active Directory Change Reporter, a Managed Object is an Active Directory domain 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 Enterprise Management Console, select the **Managed Objects** node in the left pane. The Managed Objects page will be displayed:

Figure 2: Managed Objects Page

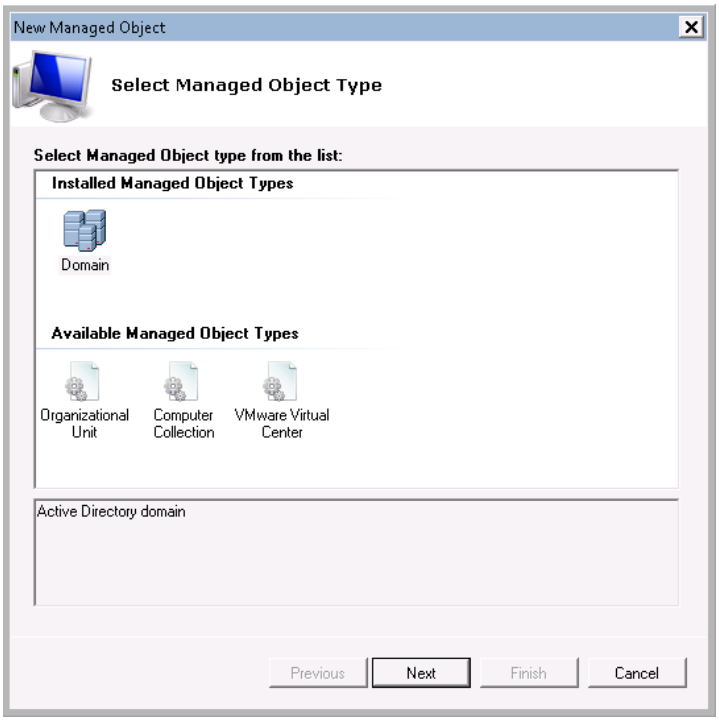
2. Click **Create New Managed Object** in the right pane. Alternatively, right-click the **Managed Objects** node and select **New Managed Object** from the popup menu to start the New Managed Object wizard.

   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 **Domain** 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 **Default Account** step, click the **Specify Account** button.

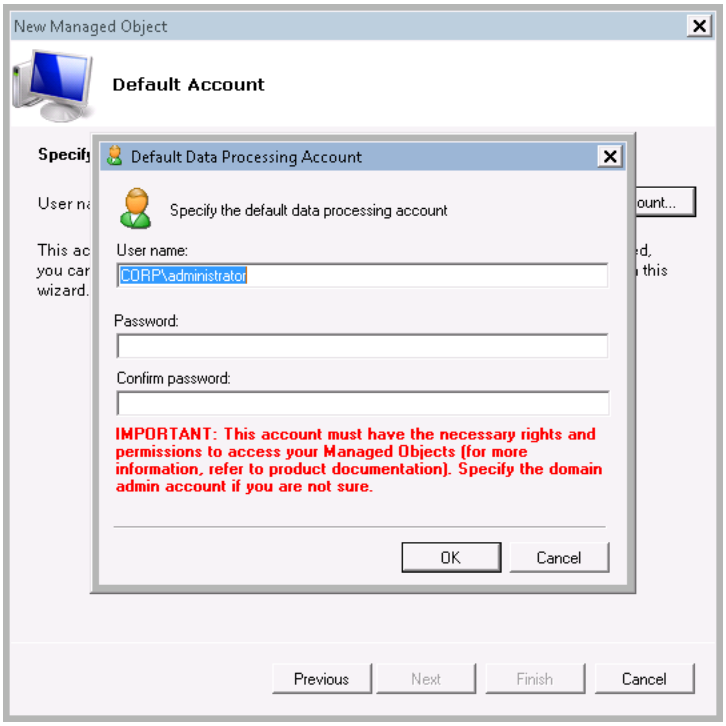
Note: If you have installed other NetWrix change reporting products before and specified the default Data Processing Account and the email settings on their configuration, the **Default Account** and **Configure Email Settings** steps of the wizard will be omitted.

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

- Local administrator on the computer where NetWrix Active Directory Change Reporter is installed.
- Domain administrator in the monitored domain. Alternatively, it must have the "Manage auditing and security log" right enabled.
- 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 detailed instructions on how to assign the "Manage auditing and security log" right and the database owner role to an account, refer to Section 6.2.1.Configuring Rights and Permissions of NetWrix Active Directory Change Reporter Installation and Configuration Guide.

Figure 4: New Managed Object: Default Account

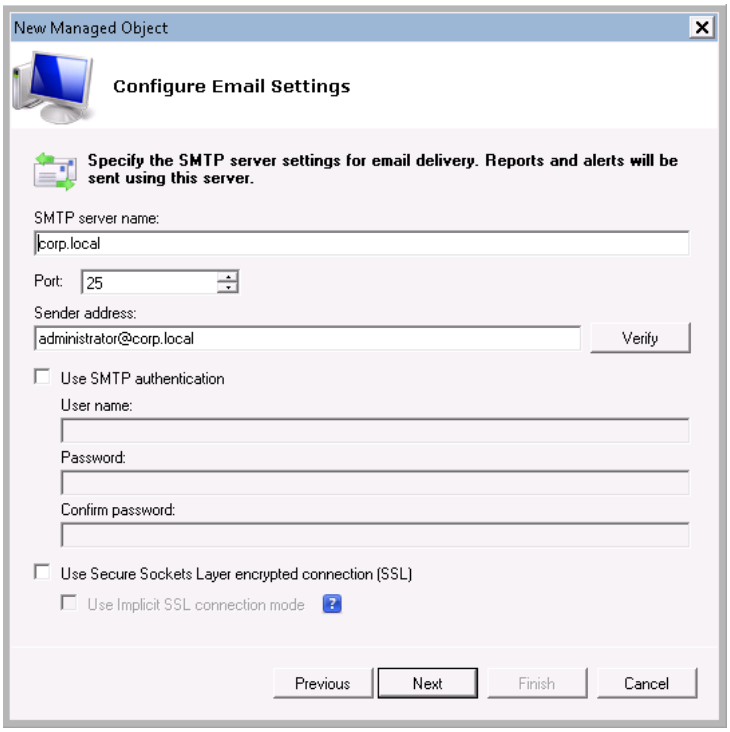


Click **OK** to continue and then **Next**.

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 29 To modify the default Data Processing Account).

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

Figure 5: New Managed Object: Configure Email Settings



The following parameters must be specified:

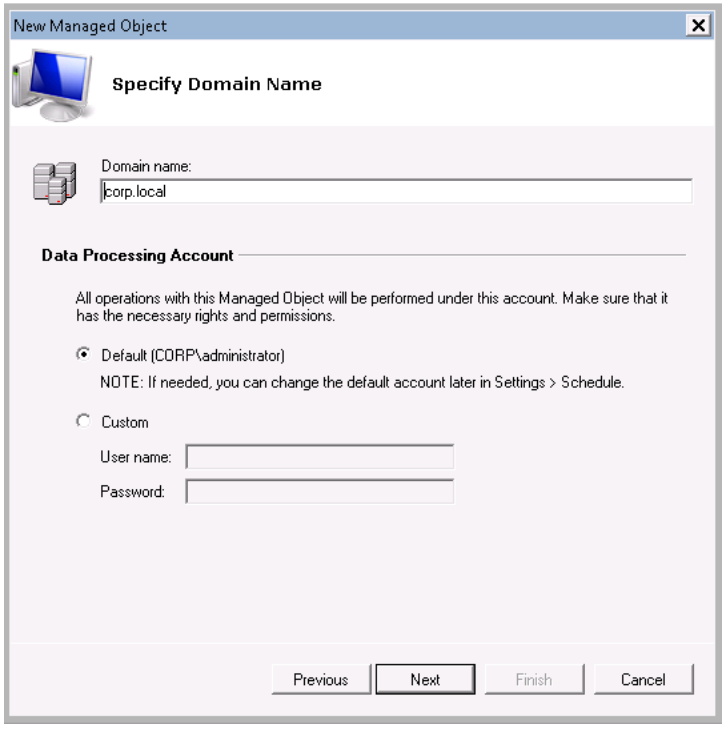
Table 2: Email Settings Parameters

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 check box 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 27 To configure the email notifications settings).

6. On the **Specify Domain Name** step, specify your domain name in the FQDN format:

Figure 6: New Managed Object: Specify Domain Name

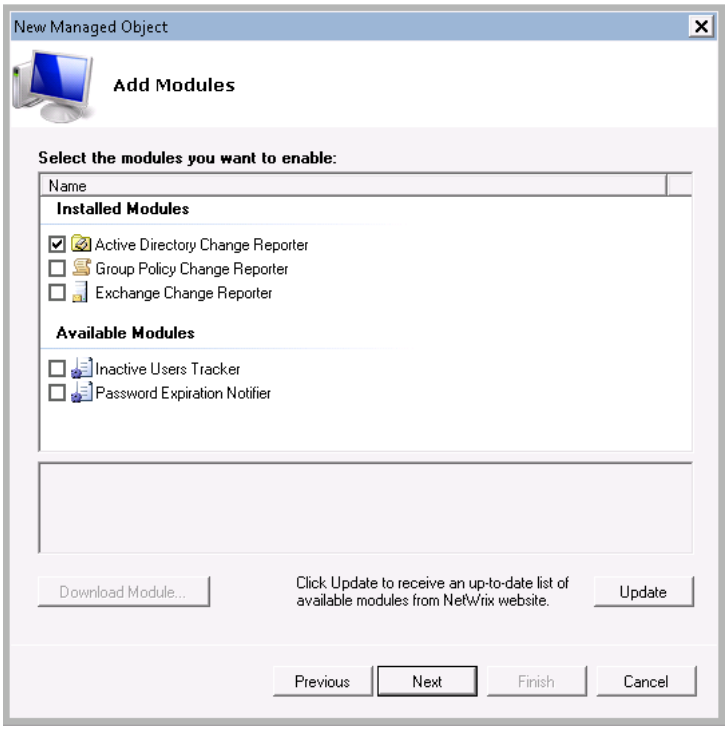


If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account earlier in this procedure), select the **Custom** option and enter the credentials. This account must be granted the

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 Active Directory Change Reporter module is selected under **Installed Modules**:

Figure 7: New Managed Object: Add Modules

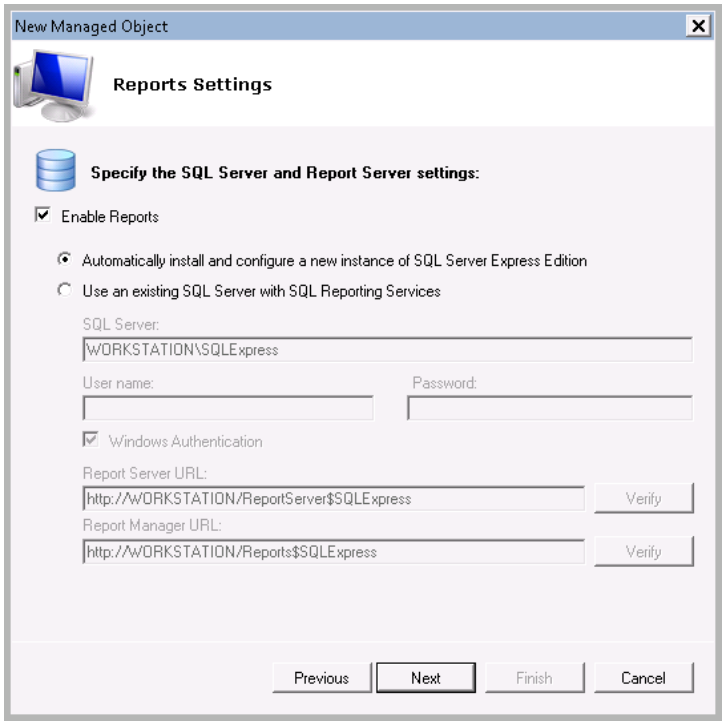


Note: If you have installed other NetWrix change reporting products before, the list of **Installed Modules** may contain several options.

On this step, under **Available Modules**, there is a list of other NetWrix products that can have domains 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 the **Download Module** button. You will be redirected to the product website page.

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

Figure 8: New Managed Object: 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 2005 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 2005 Express.
- **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 NetWrix Active Directory 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	Specify the name of the SQL Server instance name where a database of collected audit data will be created.
User name	Specify a user name for the SQL Server authentication.

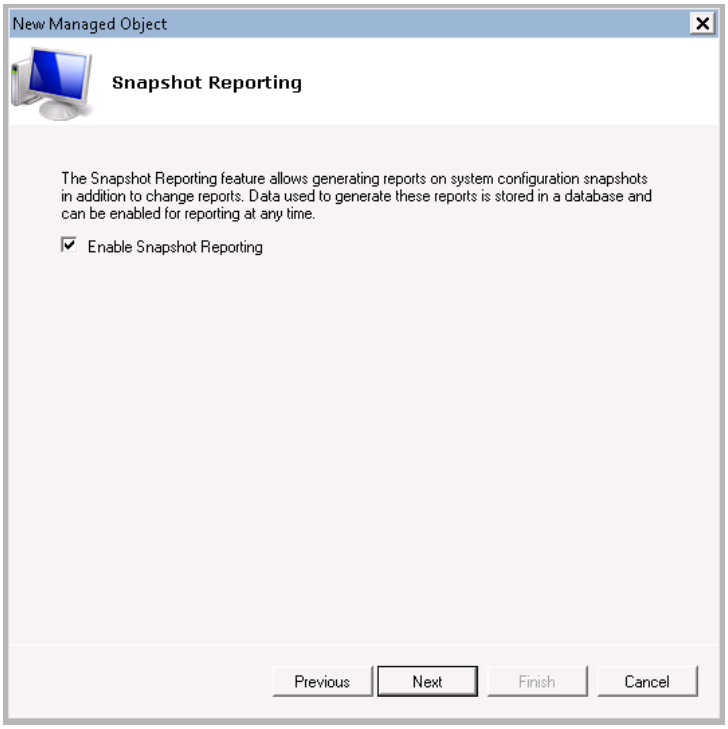
	NOTE: This user must belong to the target database owners (dbo) role. For instructions on how to assign this role to a user, refer to Section 6.2.1. Configuring Rights and Permissions of NetWrix Active Directory Change Reporter Installation and Configuration Guide.
Password	Enter a password for the SQL Server authentication.
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.
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 (e.g. 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 Enterprise Management Console has established a connection with the Report Server.

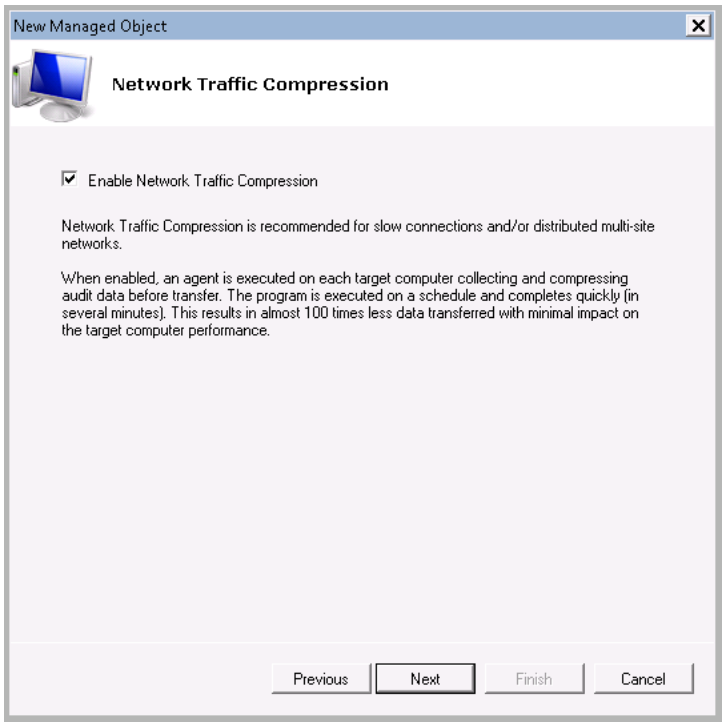
9. On the **Snapshot Reporting** step, you can enable or disable the **Snapshot Reporting** feature. It allows generating reports on your system configuration state at a specific moment of time in addition to change reports. If this feature is enabled, Active Directory snapshots will be stored in the database. This option is unavailable if the **Reports** feature is disabled. Select/deselect this option and click **Next**.

Figure 9: New Managed Object: Snapshot Reporting



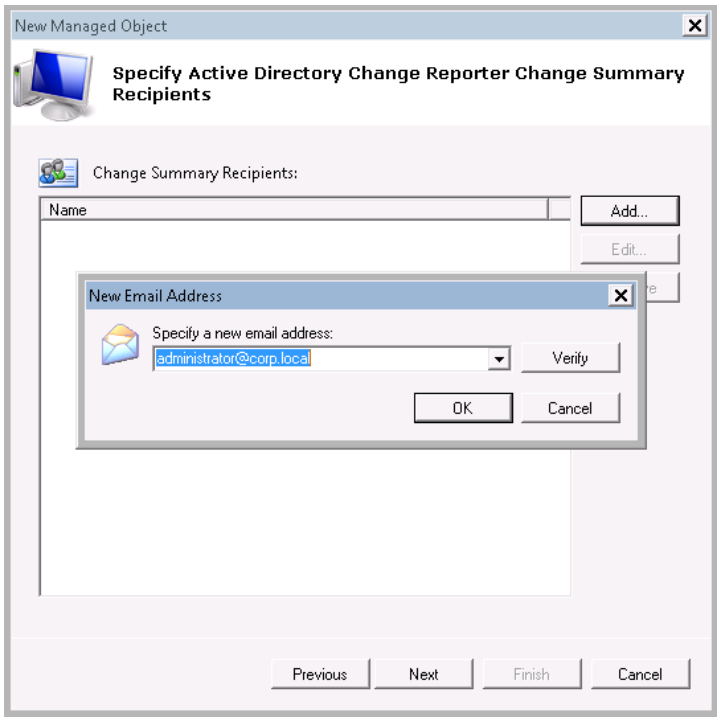
10. On the **Network Traffic Compression** step you can enable the **Network Traffic Compression** option. If this feature is enabled, an agent will be installed automatically on domain controllers in the target domain that will collect and pre-filter data and return it in a highly compressed format.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

Figure 10: New Managed Object: Network Traffic Compression



11. On the **Specify Active Directory Change Reporter Change Summary Recipients** step, click the **Add** button to specify the Change Summary recipient(s):

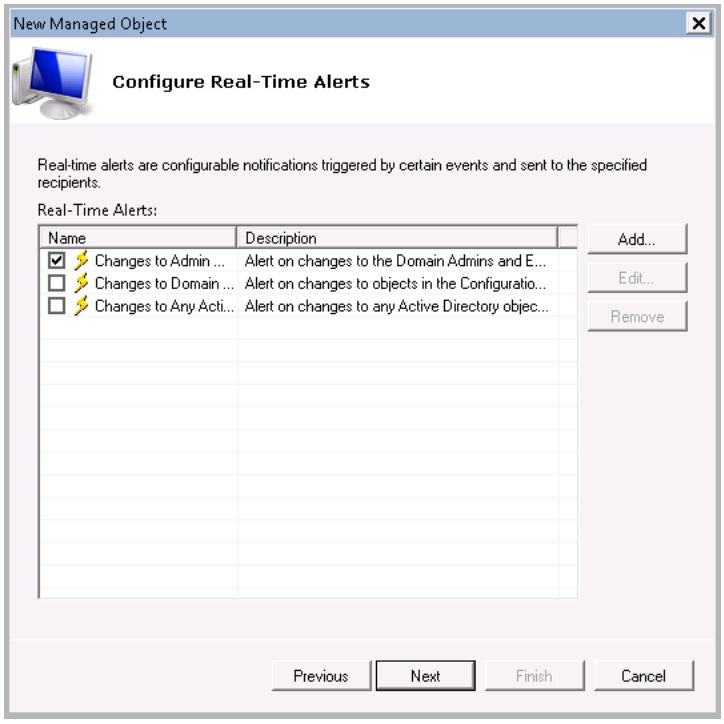
Figure 11: New Managed Object: Specify Change Summary Recipients



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. If your audit settings have not been configured properly, you will receive a warning message. For detailed instructions on how to configure audit in your monitored Active Directory domain, refer to Chapter 6. Configuring Target Environment of NetWrix Active Directory Change Reporter Installation and Configuration Guide).

12. On the **Configure Real-Time Alerts** step, you can enable or disable predefined Real-Time Alerts, or configure custom alerts by clicking the **Add** button. To enable/disable an existing alert, select/deselect the corresponding check box. For detailed instructions on how to configure a new Real-Time Alert, refer to Section 7.1 Creating Alerts. Click **Next** to continue.

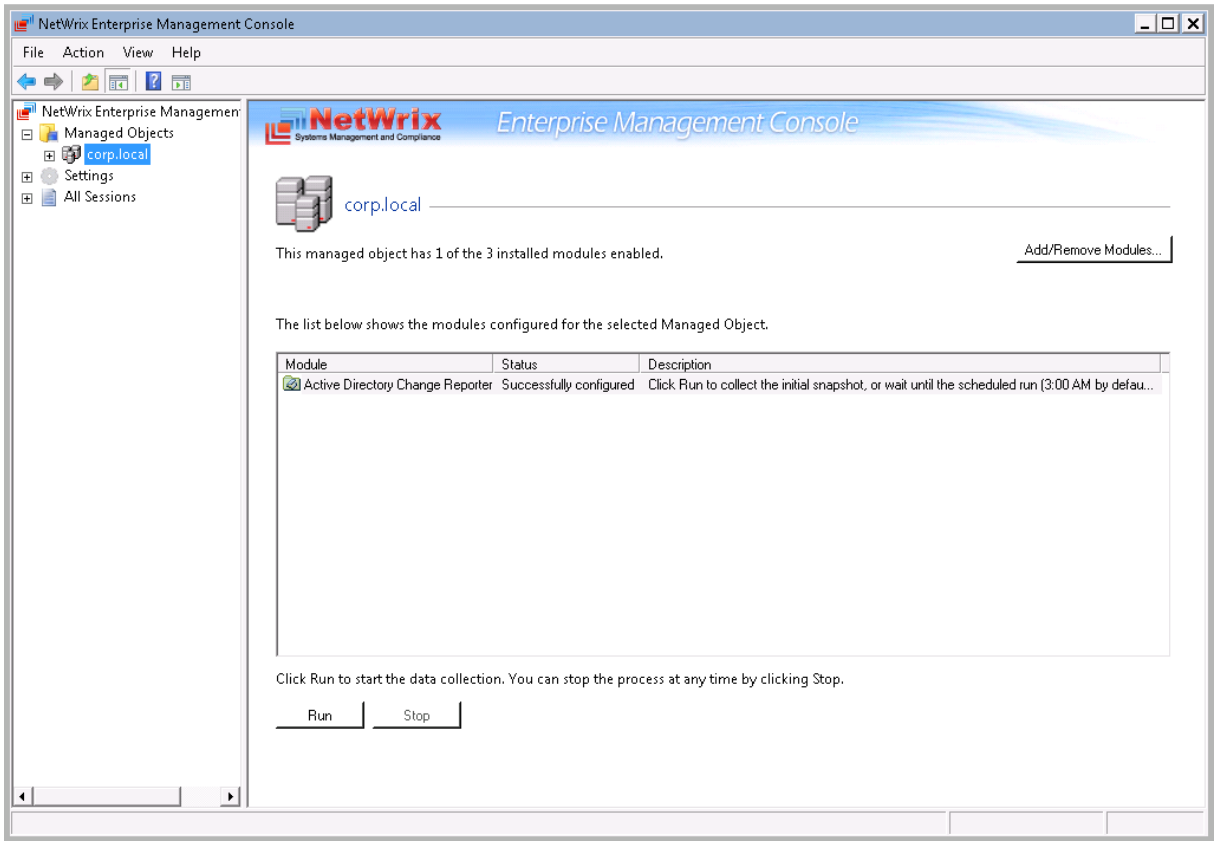
Figure 12: New Managed Object: Configure Real-Time Alerts



13. 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 13: Managed Object Page



4.2. Modifying Managed Object Settings

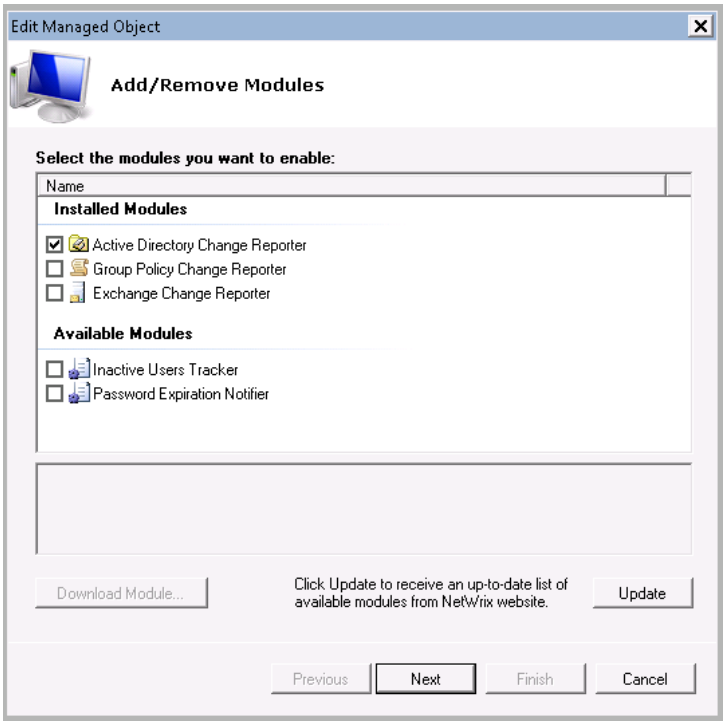
If later you need to modify the settings for an existing Managed Object, perform one of the following procedures:

- To modify general settings: add or remove NetWrix modules for the selected Managed Object.
- 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 modify Active Directory Change Reporter settings

Procedure 2. To modify general settings

1. In NetWrix Enterprise 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 14: Add/Remove Modules



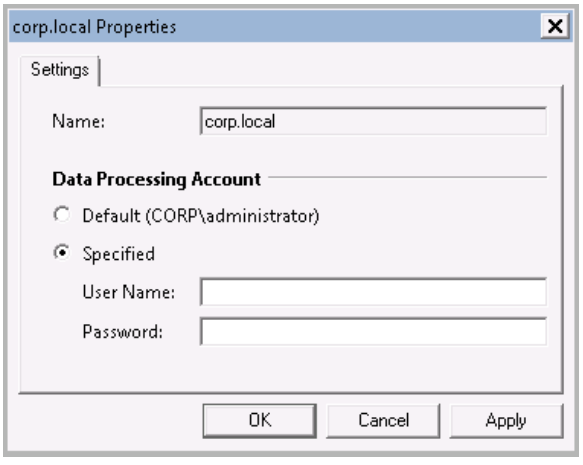
3. To add other installed modules for this Managed Object, select them from the **Installed Modules** list and click **Next**. Follow the wizard to configure the selected modules for this Managed Object.

   In this dialog, under **Available Modules**, there is also a list of other NetWrix products that can have domains 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 the **Download Module** button. You will be redirected to the product website page.

Procedure 3. To modify the Data Processing Account

1. In NetWrix Enterprise 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 **Specified** option under **Data Processing Account** and specify the credentials:

Figure 15: Managed Object Properties

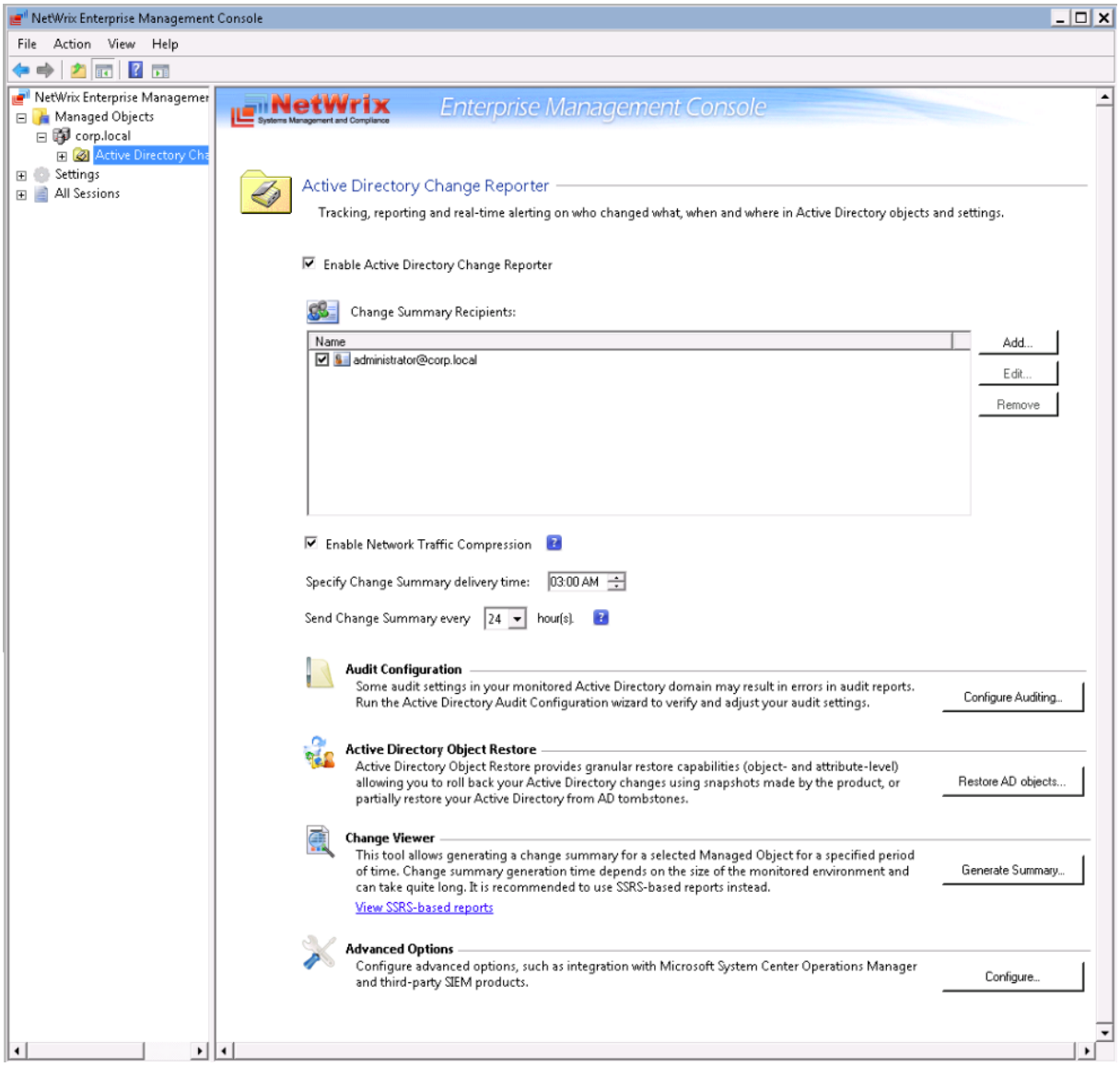


3. Click **OK** to save the changes. This account will be used for data collection from this Managed Object.

Procedure 4. To modify Active Directory Change Reporter settings

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<Managed_Object_name>** node and select Active Directory Change Reporter. The following page will be displayed:

Figure 16: Active Directory Change Reporter Page



2. To modify NetWrix Active Directory Change Reporter settings, do the following:

   - To disable (or enable, if disabled) the Active Directory Change Reporter module for this Managed Object, deselect/select the corresponding check box.
   - 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 check box.
- To modify the Change Summary delivery time (scheduled to 3:00 AM by default), set the time in the **Specify Change Summary delivery time** entry field**.**
- To modify Change Summary delivery frequency (scheduled to once a day by default), set the period (in hours) in the **Send Change Summary every x hour(s)** entry field. Change Summary will be delivered at a specified interval starting from the time indicated above.

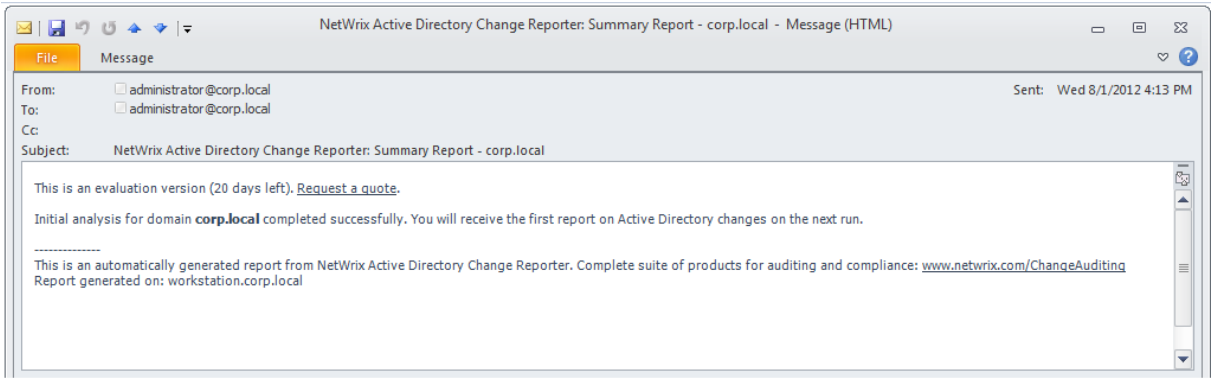
5. DATA COLLECTION

5.1. Data Collection Workflow

NetWrix Active Directory Change Reporter data collection workflow is as follows:

1. When a new Managed Object is created, NetWrix Active Directory Change Reporter starts collecting data from the monitored domain. The first data collection creates an initial snapshot of your monitored domain current state. NetWrix Active Directory Change Reporter uses this information as a benchmark to collect data on changes made to the managed domain.
2. After the initial analysis has been completed, an email notification is sent to the specified recipient(s) like in the example below:

Figure 17: Initial Analysis Notification



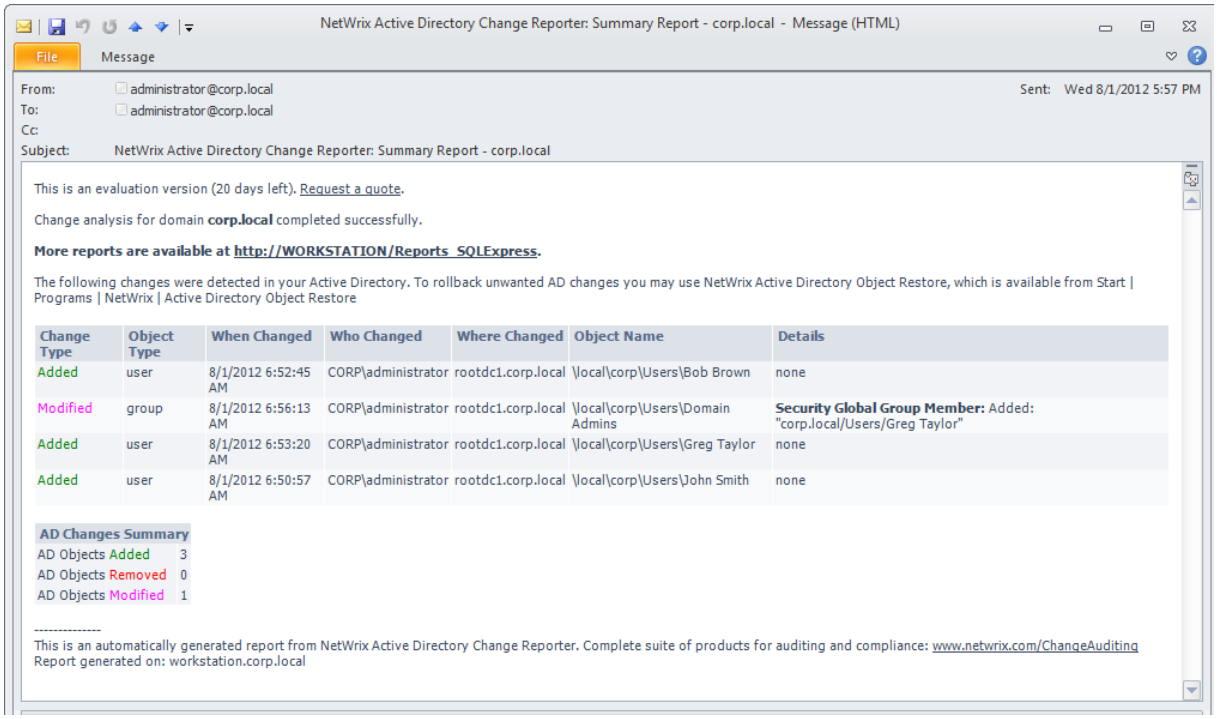
3. If NetWrix Active Directory Change Reporter detects a change that triggers a Real-Time Alert, an email notification is sent immediately to the specified recipients (for instructions on how to configure Real-Time Alerts, refer to Chapter 7 Real-Time Alerts).
4. Once a day (at 3:00 AM by default), NetWrix Active Directory Change Reporter writes data on detected changes to a local storage of audit data, the Audit Archive. If the Reports feature is enabled and configured, data is then imported from the Audit Archive to a SQL database. If the Snapshot Reporting feature is enabled, the product will also write data on the monitored domain configuration state.
5. 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 5.2.1 Modifying Change Summary Delivery Schedule).

Note: For NetWrix Active Directory Change Reporter to be able to collect audit data successfully, you need to configure your monitored Active Directory domain for audit prior to using the product. For detailed instructions on how to do this, refer to Chapter 6. Configuring Target Environment of NetWrix Active Directory Change Reporter Installation and Configuration Guide.

5.2. Change Summary

By default, a Change Summary is emailed to the specified recipients daily at 3:00 AM and contains the information on changes that occurred in the last 24 hours:

Figure 18: Change Summary Example



It provides the following information:

Table 4: Change Summary Fields

Parameter	Description
Change Type	Shows the type of action that was performed on the AD object. The possible values are: • Added • Removed • Modified
Object Type	Shows the type of the AD object that was changed, e.g. "user".
When Changed	Shows the exact time when the change occurred.
Who Changed	Shows the name of the account under which the change was made.
Where Changed	Shows the name of the domain controller where the change was made.
Object Name	Shows the path to the AD object that was changed.
Details	Shows the before and after values for the modified object.

5.2.1. Modifying Change Summary Delivery Schedule

To modify the Change Summary delivery schedule, do the following:

Procedure 5. To modify Change Summary delivery schedule

1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter** (see Figure 16: Active Directory Change Reporter Page).

2. In the right pane, set the time for the Change Summary delivery in the **Specify Change Summary delivery time** entry field.
3. If you wish to receive the Change Summary more frequently than once a day, modify the default value in the **Send Change Summary every x hour(s)** entry field. The Change Summary will be delivered at a specified interval starting from the time indicated above.

5.2.2. Generating Change Summary on Demand

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

Procedure 6. To generate Change Summary on Demand

1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** (see Figure 13: Managed Object Page).
2. In the right pane, 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.

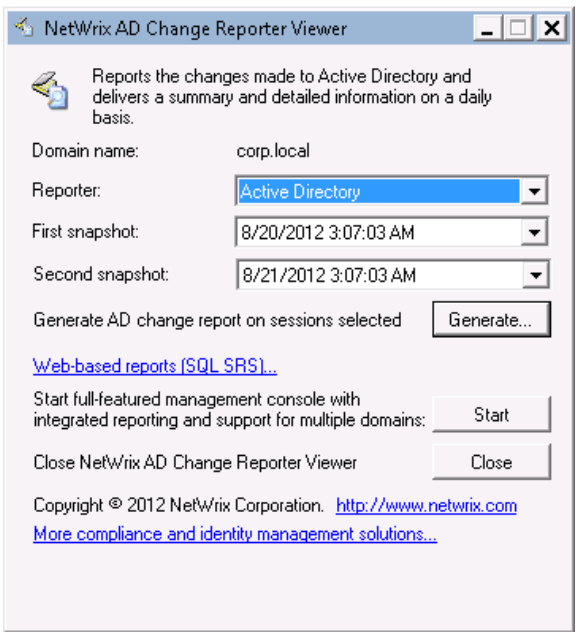
5.2.3. Viewing Change Summary for a Specified Date Range

If you want to generate a Change Summary for a specific date range, do the following:

Procedure 7. To generate Change Summary for a specific date range

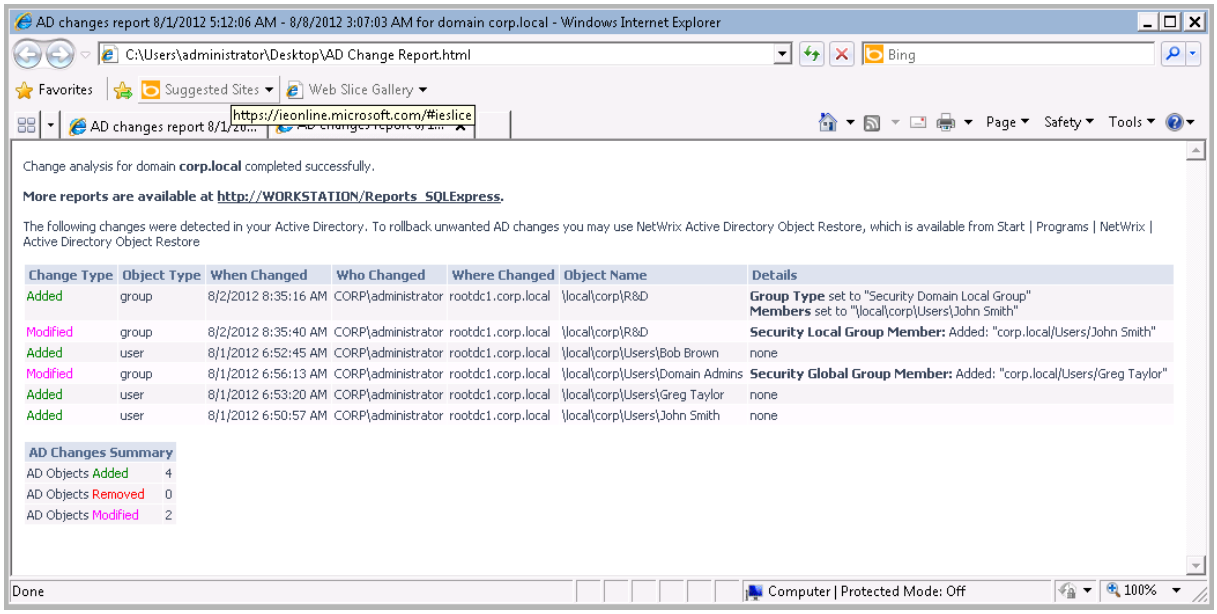
1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter** (see Figure 16: Active Directory Change Reporter Page).
2. In the right pane, click the **Generate Summary** button next to **Change Viewer**. The Change Viewer tool will open:

Figure 19: NetWrix Active Directory Change Reporter Viewer



3. Select **Active Directory** from the drop-down list under **Reporter**.
4. Specify the date range by selecting NetWrix Active Directory Change Reporter snapshots in the **First snapshot** and **Second snapshot** drop-down lists.
5. Click the **Generate** button. In the **Save as** dialog, specify the target location for the Change Summary. Once generated, it will be displayed in your default web browser:

Figure 20: Change Summary for a Specific Date Range



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.

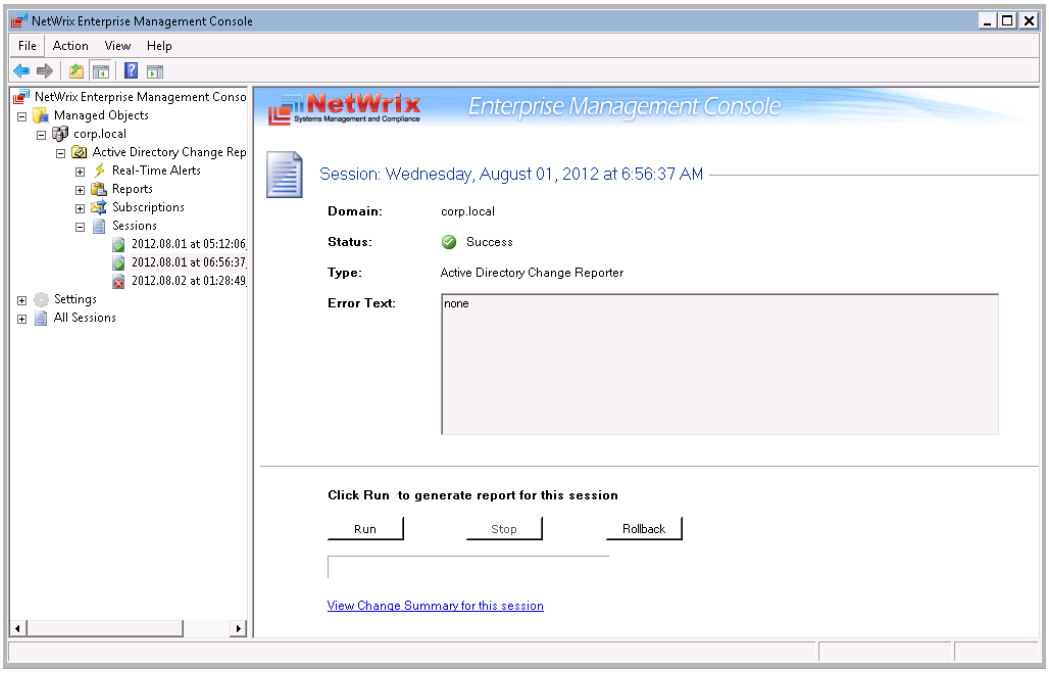
5.3. Sessions

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 Enterprise Management Console navigate to **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter** → **Sessions**.
- In bulk for all Managed Objects and installed modules: in NetWrix Enterprise 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 21: Session Page



The following information is provided:

Table 5: Session Details

Parameter	Description
Domain	Shows the name of the monitored domain.
Status	Shows Session status. The possible values are Success and Error.
Type	Shows the NetWrix module that this Session is for.
Error Text	Displays an error text if the Session status is Error.

From this page, you can also view a Change Summary for a particular Session in a web browser, and rollback unwanted changes to Active Directory objects. For detailed instructions on how to perform these tasks, refer to Section 5.3.1 Viewing Change Summary for Sessions and Chapter 8 Active Directory Object Restore respectively.

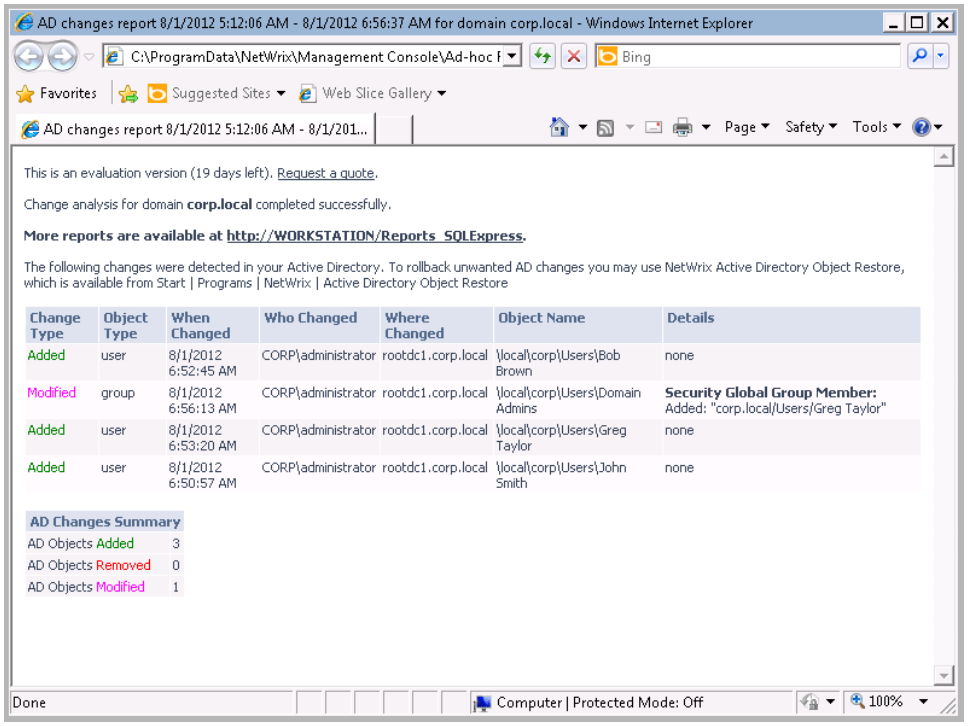
You can configure the number of Sessions available for review in NetWrix Enterprise Management Console by specifying the date range for Sessions to be stored. For detailed instructions on how to do this, refer to Section 9.3 Configuring Audit Archive Settings.

5.3.1. Viewing Change Summary for Sessions

Procedure 8. To view Change Summary for a Session

1. Select a Session that you want to view the Change Summary for.
2. In the right pane, click the **Run** button to generate the Change Summary. If you have already generated the Change Summary for this session before, click the **View Change Summary for this session** link.
3. The Change Summary for this session will be displayed in your default web browser:

Figure 22: Web-based Change Summary Example



6. REPORTS

6.1. Reports Overview

NetWrix Active Directory Change Reporter allows generating reports based on Microsoft SQL Server Reporting Services (SSRS). The product provides a wide variety of predefined report templates that will help you stay compliant with various standards and regulations (GLBA, HIPAA, PCI, SOX, 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 Active Directory Change Reporter, three types of reports are available:

- AD Snapshot Reports: allow generating reports on your AD domain configuration state at a specific moment of time in addition to change reports. These reports are only available if the Snapshot Reporting feature is enabled. For detailed information on Snapshot Reports, refer to Section 6.5 Snapshot Reporting of this guide.
- All Changes Reports: show a summary of all Active Directory changes filtered by different parameters (date, user and so on) and in different formats (table or chart).
- Best Practice Reports: show the information most commonly required for audit purposes.

For a full list of available reports, expand the corresponding node under **Managed Objects → <Managed_Object_name> → Active Directory Change Reporter → Reports**:

Figure 23: 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 SRS Server
- Import audit data from the Audit Archive to a SQL database
- Assign permissions to view web-based reports

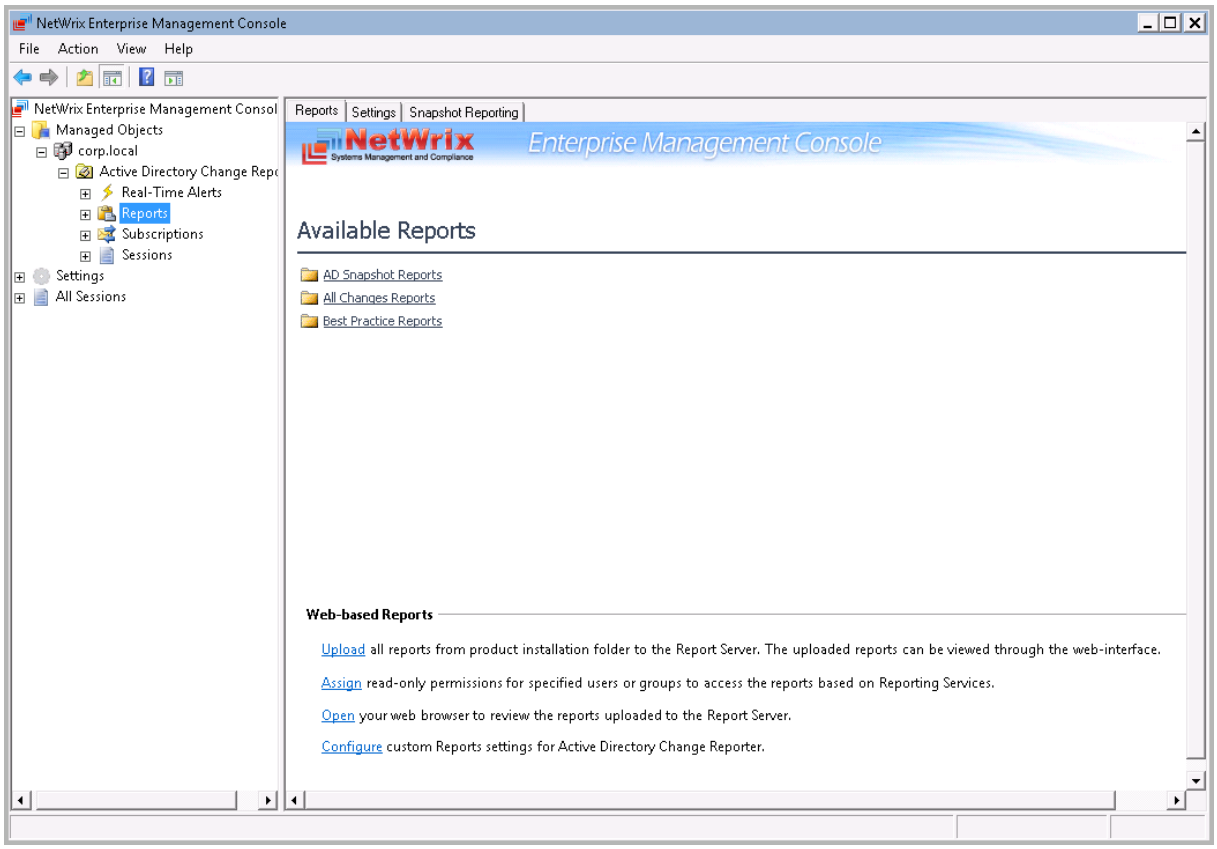
6.2.1. Specifying SQL Server Settings

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 9. To configure Reports

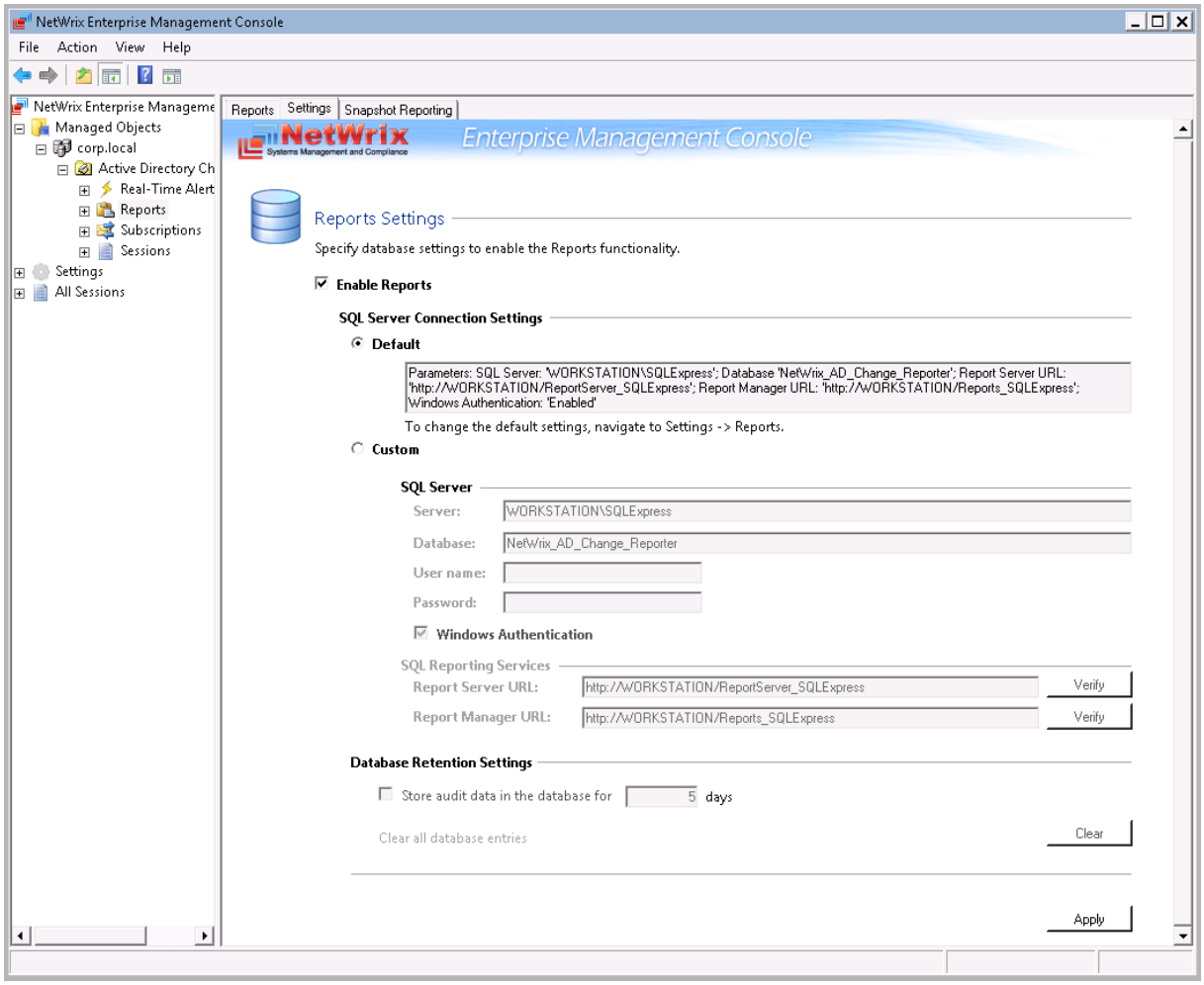
1. In NetWrix Enterprise Management Console, expand the **Managed Object** → **<Managed_Object_name>** → **Active Directory Change Reporter** node and select **Reports**. The following page will be displayed:

Figure 24: Reports Page



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

Figure 25: Reports Settings



3. Specify/modify the following parameters:

Table 6: Reports Settings

Parameter	Description
Enable Reports	Select this check box 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 a user to access the SQL Server. This user must belong to the target database owner role.
Password	Specify a 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	This option is disabled in this product version
Clear all database entries	Click the **Clear** button if you want to delete all data from the SQL database.

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

Note: When you configure the Reports settings, a SQL database for audit data is created. If you skip the Reports configuration on a 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 decide to enable the Reports feature for this 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 using the DB Importer tool. For detailed instructions on how to do this, refer to Section 6.2.3 Importing Audit Data to SQL Database of this guide.

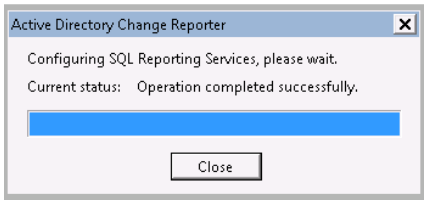
6.2.2. Uploading Report Templates to the Report Server

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 10. To upload report templates to the Report Server

- On the Reports page (see Figure 24: 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 26: Uploading Report Templates



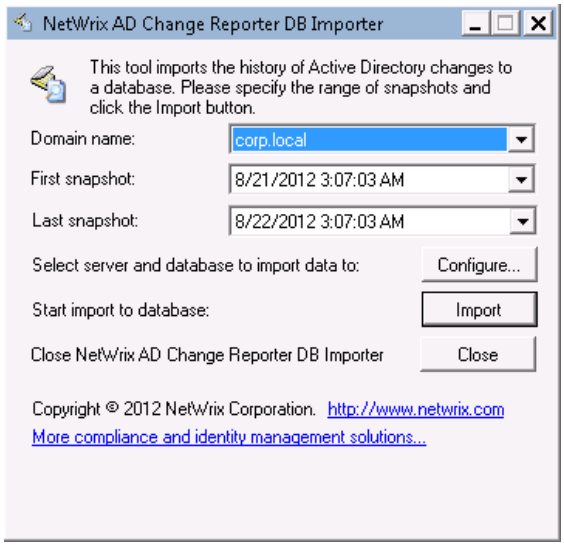
6.2.3. Importing Audit Data to SQL Database

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 11. To import audit data

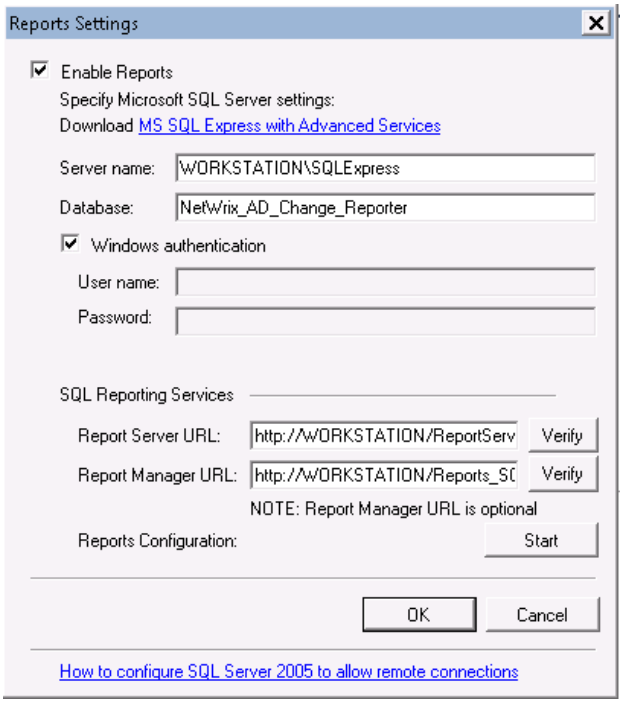
1. Navigate to **Start** → **All Programs** → **NetWrix** → **Active Directory Change Reporter** → **Advanced Tools** and select DB Importer. The DB Importer dialog will open:

Figure 27: NetWrix DB Importer



2. Select your monitored domain under **Domain name** and the time range for which you want to import data from the **First snapshot** and **Last snapshot** drop-down lists.
3. Click the **Configure** button to select the target database. The following dialog will be displayed with the default SQL Server and Report Server Settings:

Figure 28: Reports Settings



4. Verify the database settings and click **OK**.
5. 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.

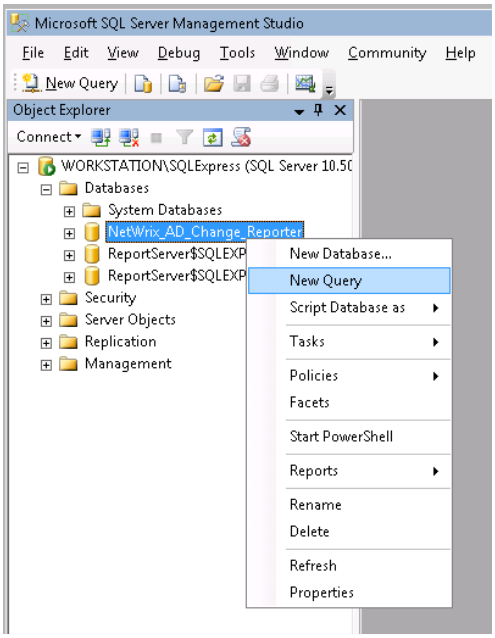
6.2.4. Configuring Audit Database Retention Policy

If you want audit data to be deleted automatically from your SQL database after a certain period of time, you can specify the retention policy for audit data.

Procedure 12. To configure audit database retention period

1. Navigate to **Start → All Programs → Microsoft SQL Server → SQL Server Management Studio** and connect to your SQL Server instance.
2. In the left pane, navigate to your target database, right-click it and select **New Query** from the popup menu:

Figure 29: Create New Query

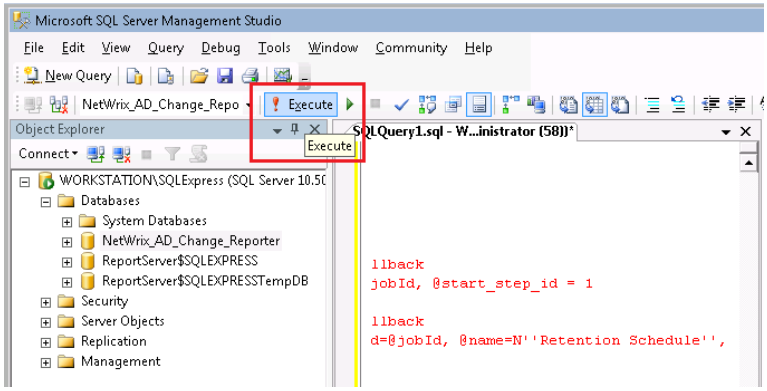


3. Copy the script contained in Appendix B: Appendix: SQL Database Retention Script of this document and paste it into the **Query** tab.
4. In the second line of the query, specify the retention period for your audit data in days:

```
SET @Retention_Period_Days = 90
```

5. Click **Execute** in the Microsoft SQL Server Management Studio toolbar to execute the query:

Figure 30: Execute Query



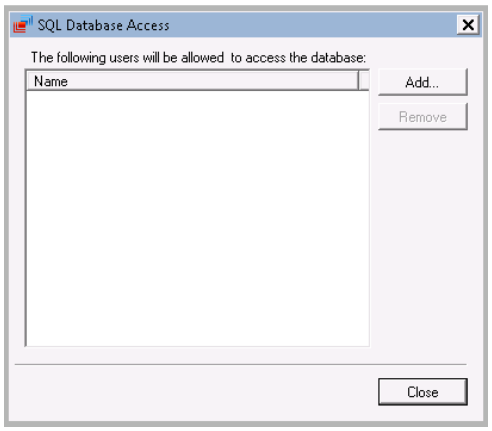
6.2.5. Assigning Permissions to View Reports

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 13. To assign permissions to view reports

1. On the Reports page (see Figure 24: Reports Page), click **Assign** under **Web-based Reporting**. The following dialog will be displayed:

Figure 31: 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 Active Directory Change Reporter provides two options for viewing reports:

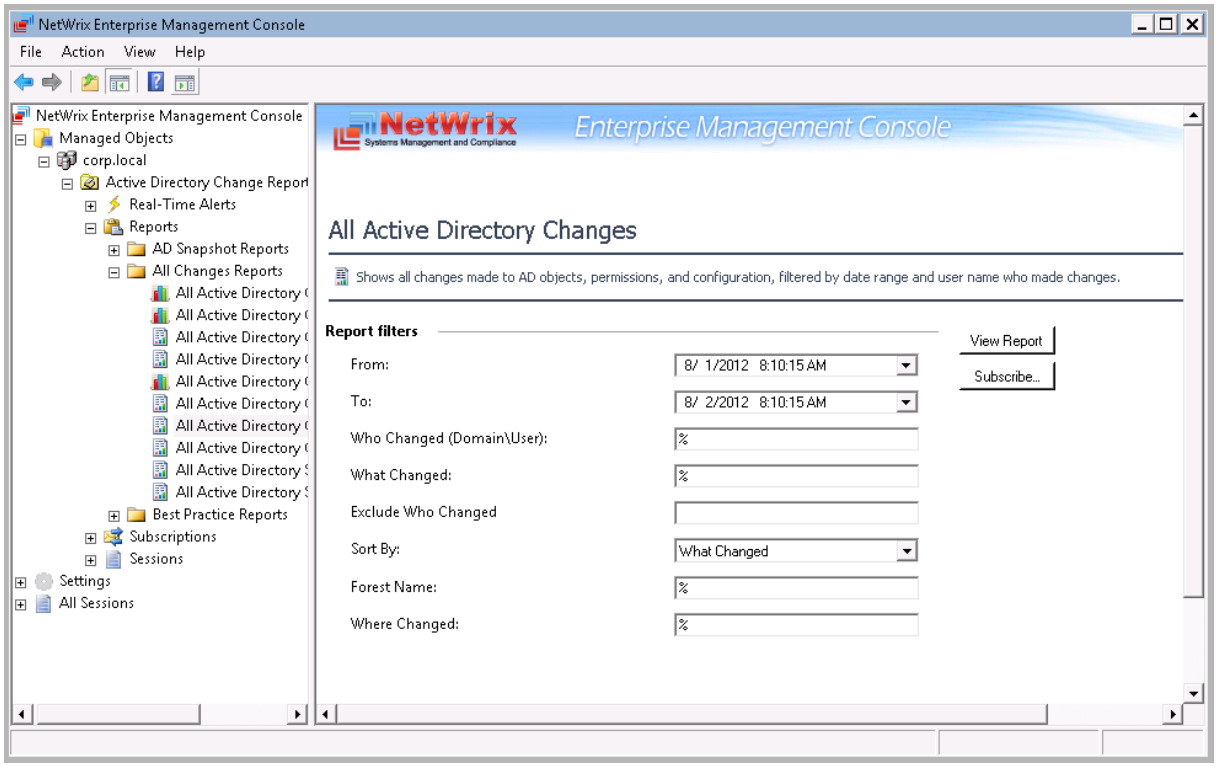
- In NetWrix Enterprise Management Console
- In a web browser

6.3.1. Viewing Reports in NetWrix Enterprise Management Console

Procedure 14. To view a report in NetWrix Enterprise Management Console

1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** → **Active Directory 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 32: All Active Directory Changes 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 33: All Active Directory Changes Report (Console)

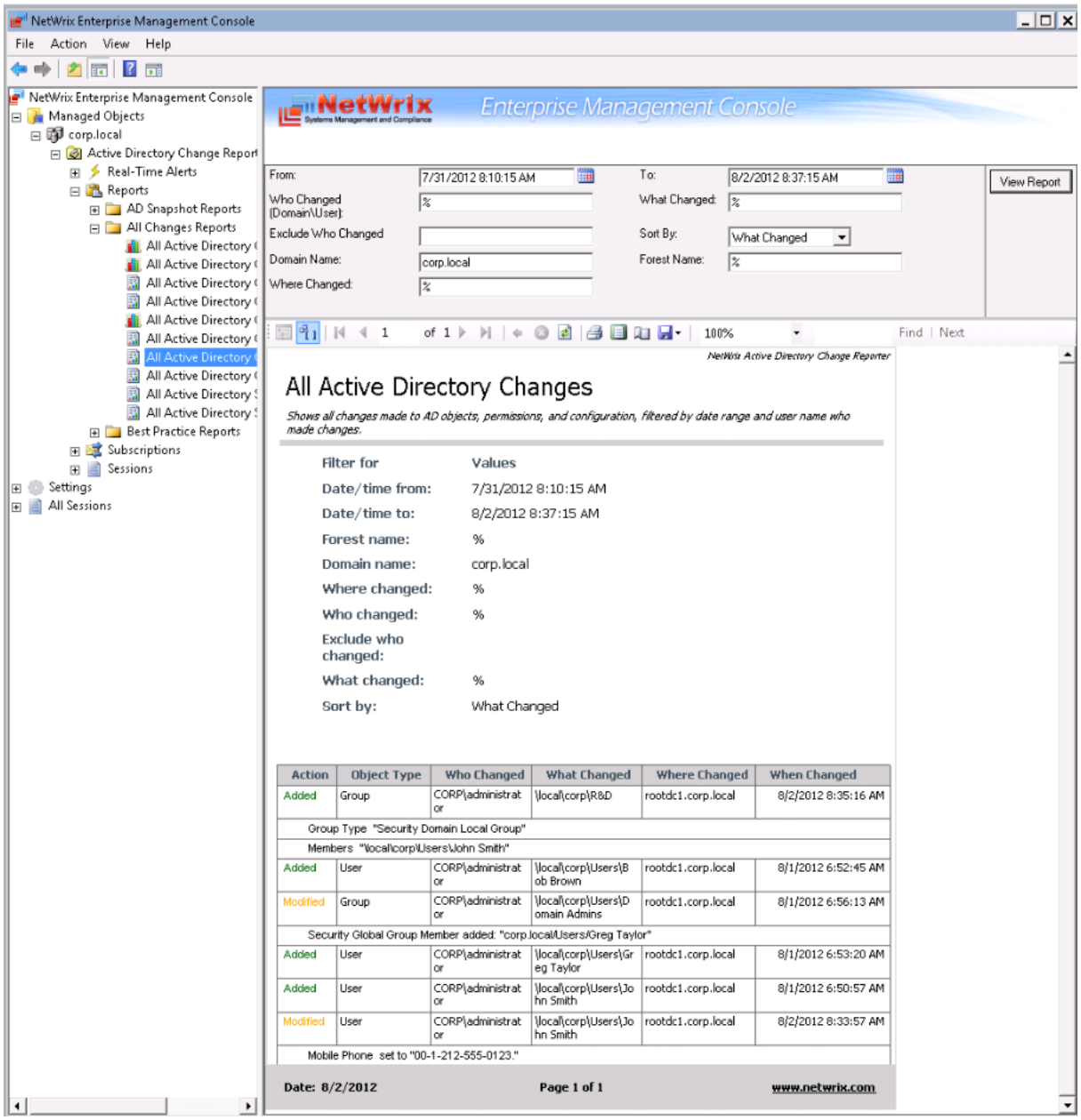
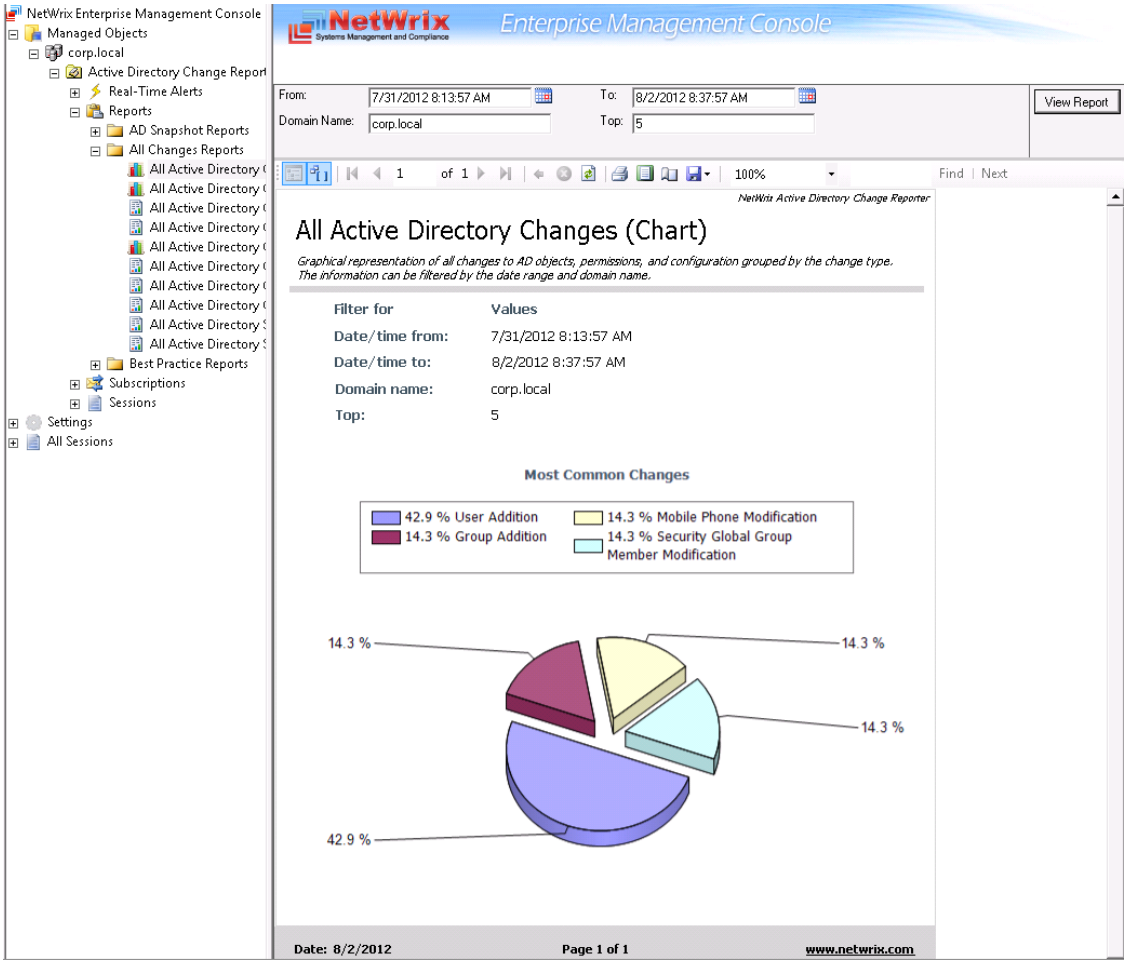


Chart reports provide a visual representation of the changes statistics in the monitored domain:

Figure 34: All Active Directory Changes Chart Report (Console)



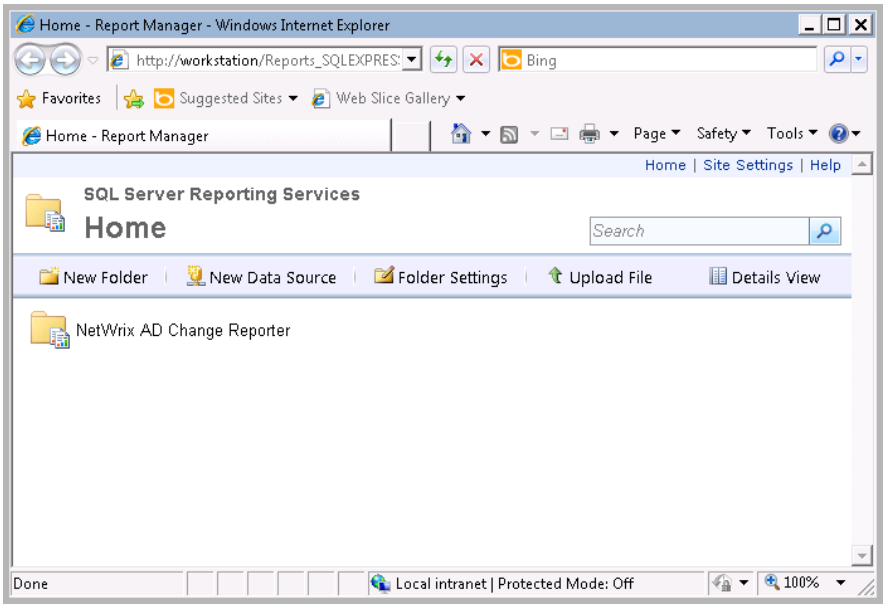
6.3.2. Viewing Reports in a Web Browser

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

Procedure 15. 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 Enterprise Management Console by navigating to **Settings** → **Reports**). Alternatively, in NetWrix Enterprise Management Console, navigate to the Reports page (see Figure 24: Reports Page) and click **Open** under **Web-based Reports**. The following page will be displayed:

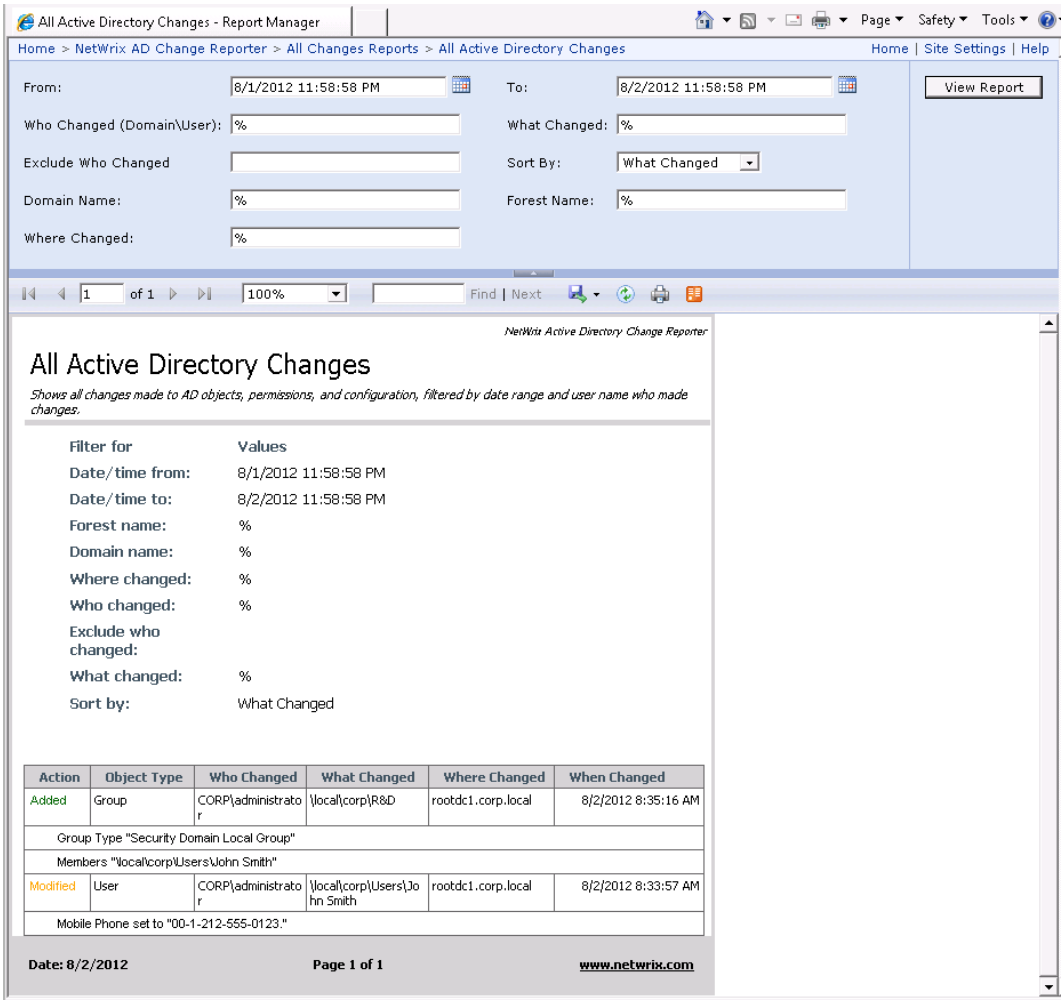
Figure 35: SQL Server Reporting Services Page



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 AD 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:

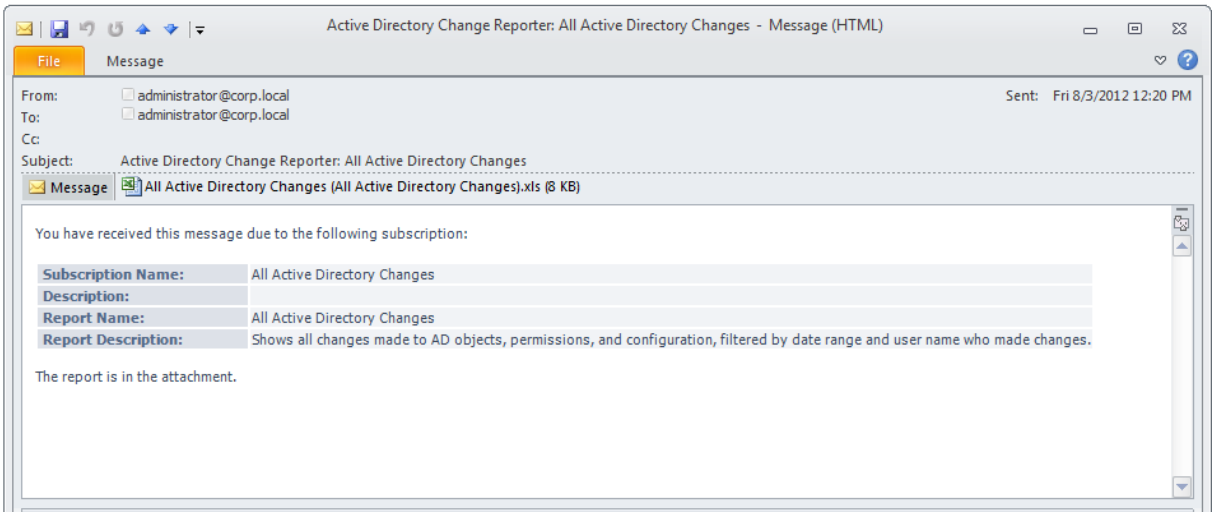
Figure 36: All Active Directory Changes Report (Web Browser)



6.4. Configuring Report Subscriptions

In NetWrix Active Directory 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 37: Report Delivered by Subscription



This section provides detailed instructions on how to:

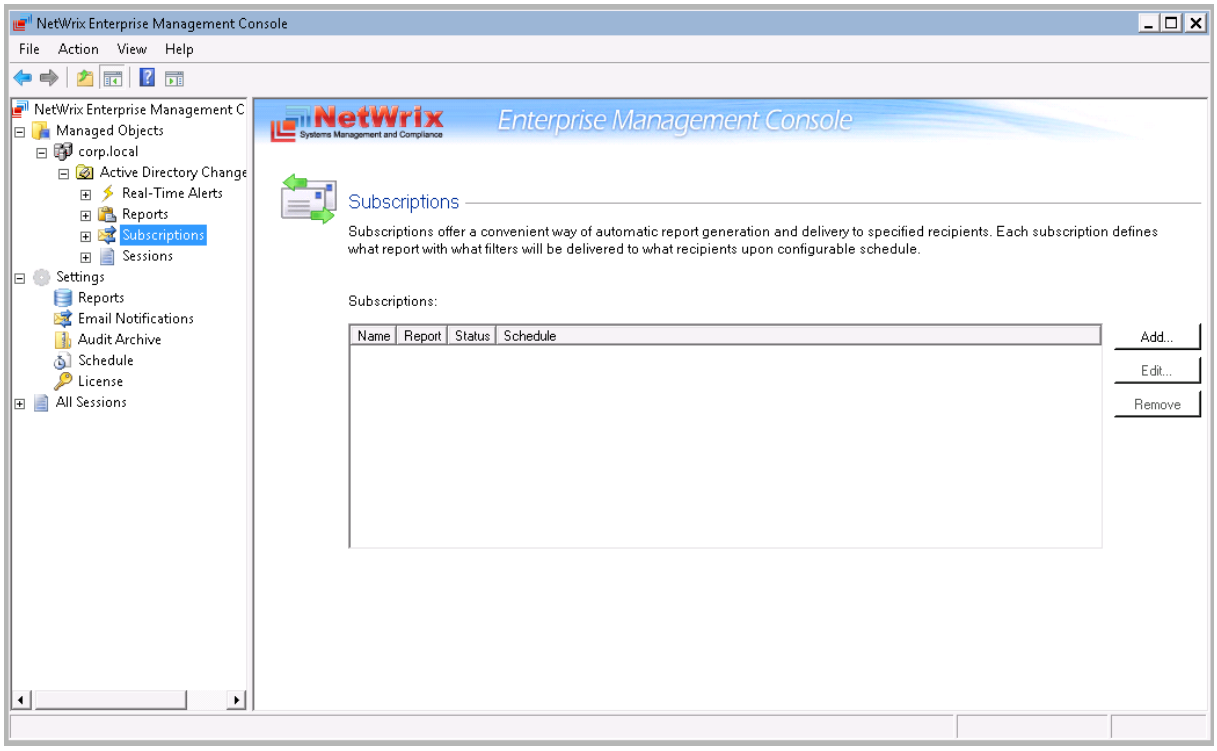
- Create a Subscription
- Modify a Subscription
- Force on-demand report delivery

6.4.1. Creating a Subscription

Procedure 16. To create a Subscription

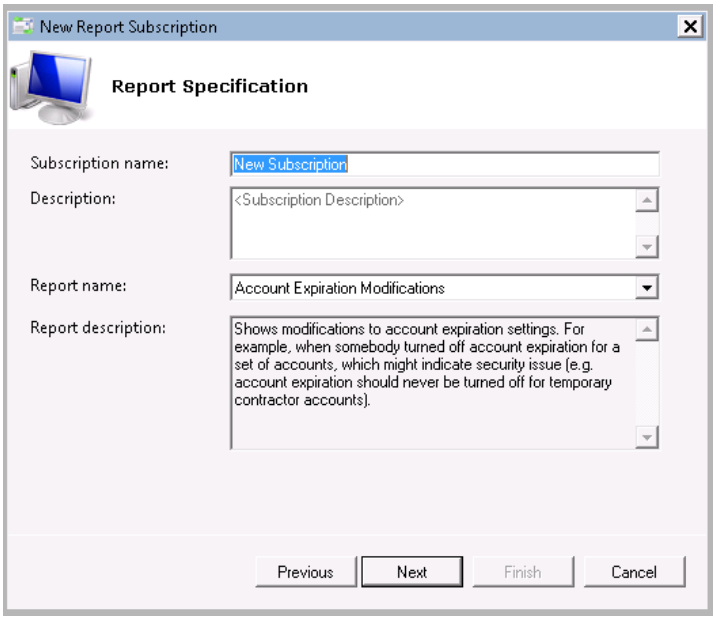
1. In NetWrix Enterprise Management Console, navigate to **Managed Objects → <Managed_Object_name> → Active Directory Change Reporter → Subscriptions**. The following page will be displayed:

Figure 38: 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 following dialog will be displayed:

Figure 39: Report Specification



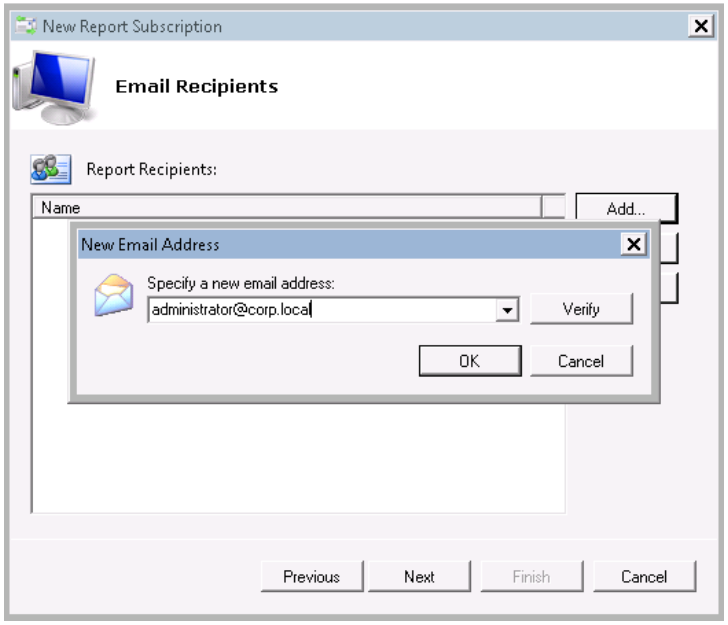
4. Specify the following parameters and click **Next** to proceed:

Table 7: Subscription Settings

Parameter	Description
Subscription name	Specify the subscription name. This name will be displayed in NetWrix Enterprise 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.

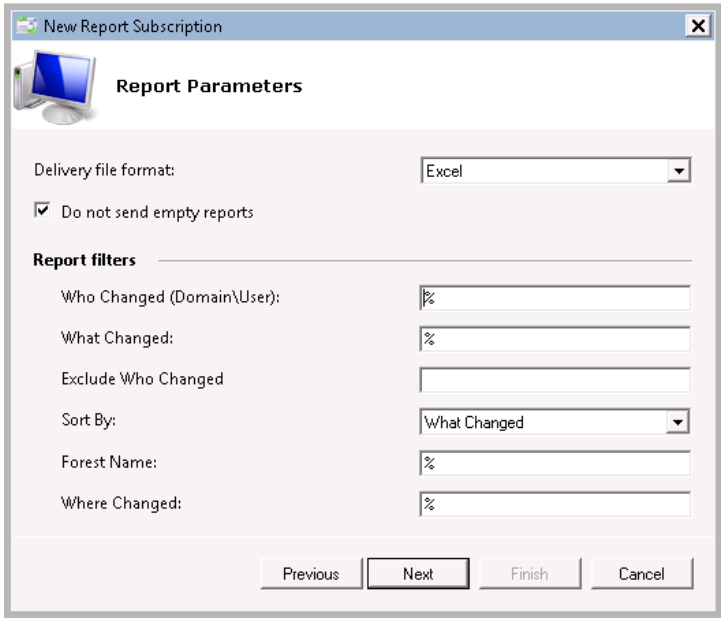
5. On the **Email Recipients** step, click the **Add** button and specify the email address(es) of the report recipients. It is recommended to click the **Verify** button. The system will send a test message to the specified address and will inform you if any problems are detected. Click **OK** to add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

Figure 40: Report Subscription Wizard: Specify Recipients



6. On the **Report Parameters** 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.

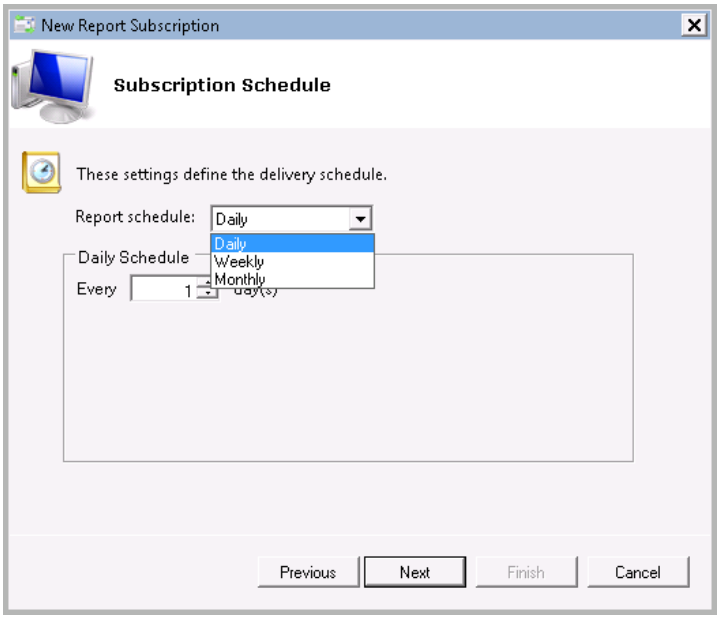
Figure 41: Report Subscription Wizard: Report Parameters



7. On the **Subscription 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.

Figure 42: Subscription 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.

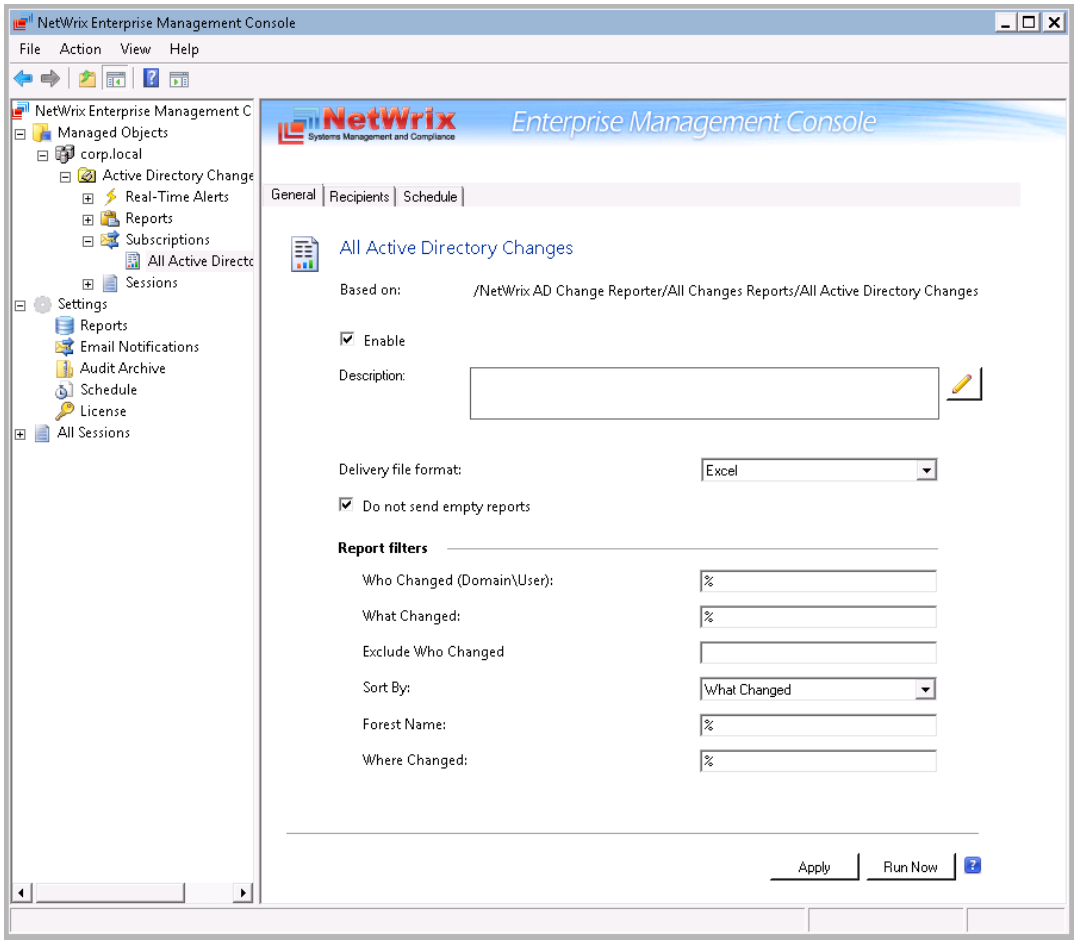
6.4.2. Modifying a Subscription

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

Procedure 17. To modify a Subscription

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter** → **Subscriptions** node and select the Subscription you want to modify. The Subscription page will be displayed:

Figure 43: Subscription Page



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

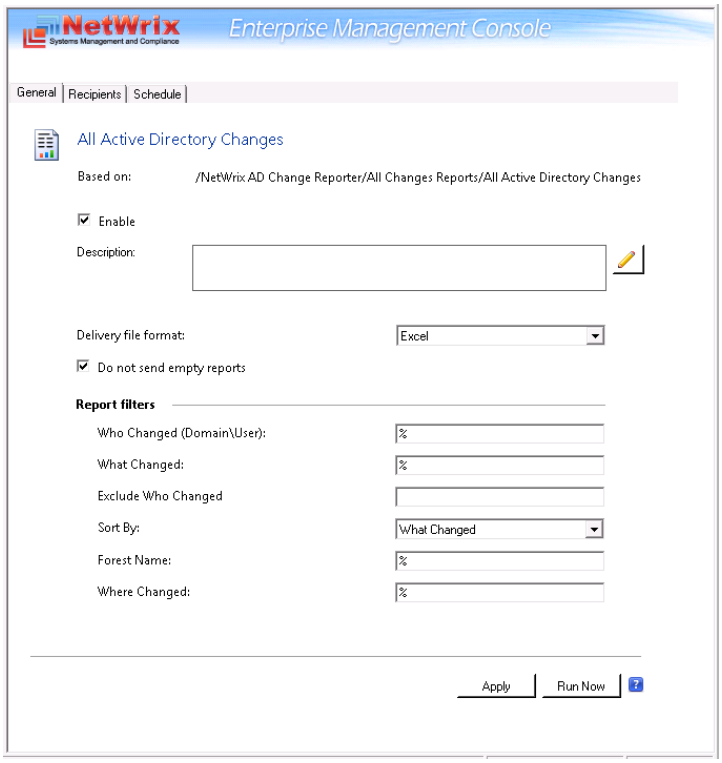
6.4.3. Forcing On-Demand Report Delivery

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

Procedure 18. To force on-demand report delivery

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<Managed_Object_name>** → **Active Directory 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**:

Figure 44: Report 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. Snapshot Reporting

The Snapshot Reporting feature allows generating reports on your AD domain configuration state at a specific moment of time in addition to change reports.

Like all other NetWrix Active Directory Change Reports, Snapshot Reports can be viewed in NetWrix Enterprise Management Console or in a web browser. You can also subscribe to Snapshot Reports in the same way as to other repot types (for detailed instructions, refer to Section 6.4 Configuring Report Subscriptions).

This section provides detailed instructions on how to:

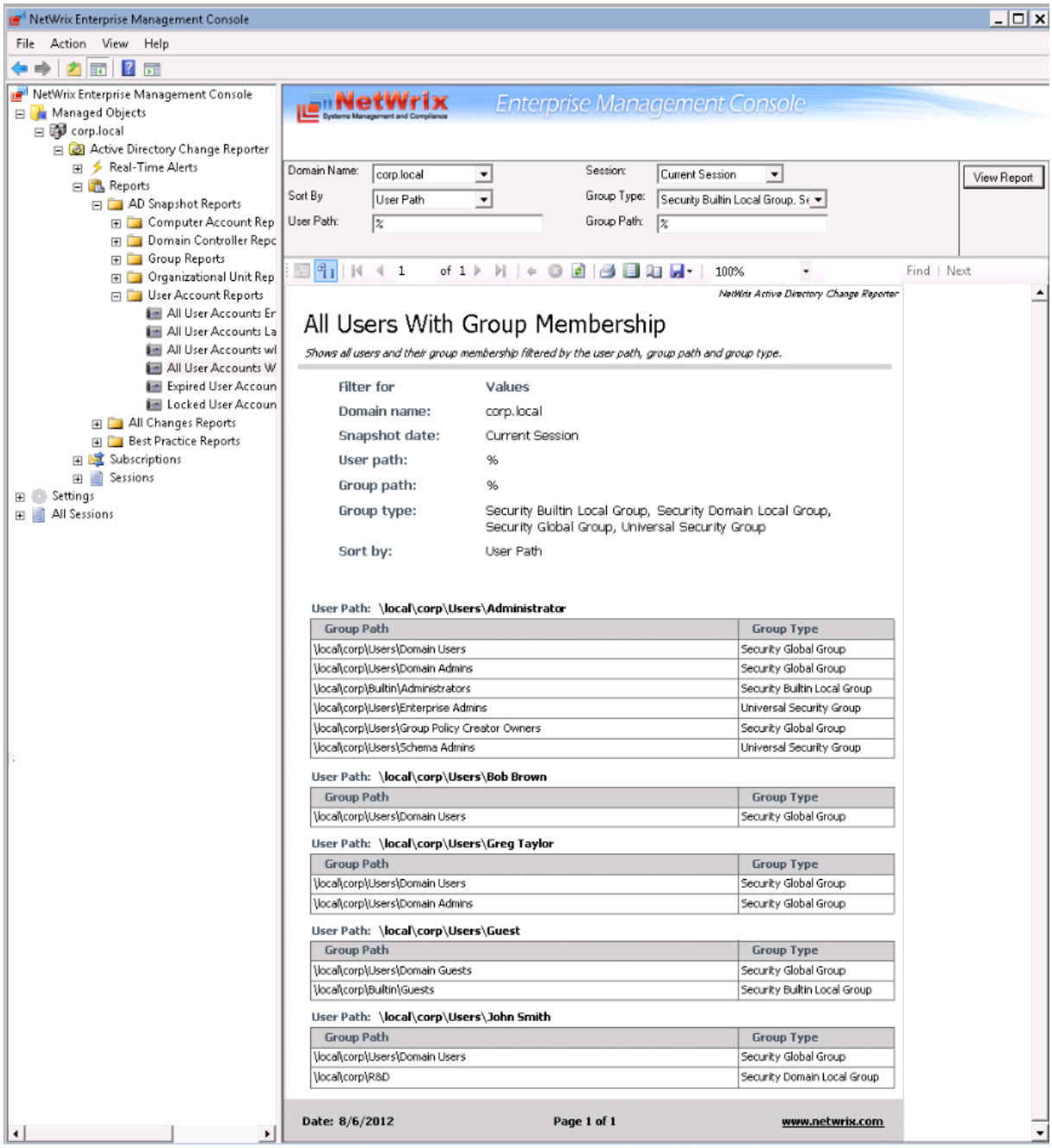
- View Snapshot Reports
- Import historical snapshots to the database

6.5.1. Viewing Snapshot Reports

Procedure 19. To view Snapshot Reports

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter** → **Reports** → **AD Snapshot Reports** node.
2. Select the report you want to generate and specify the report filters.
3. Click the **View Report** button and wait for the report to be generated:

Figure 45: Snapshot Report: All Users With Group Membership



By default, Snapshot Reports display the current configuration state of your monitored domain. If you want to generate a report on a different snapshot, select it from the **Session** filter.

Note: To be able to generate reports on different snapshots, you need to import them to the database. Otherwise, only the Current Session option is available. For detailed instructions on how to import snapshots, refer to Section 6.5.2 Importing Historical Snapshots.

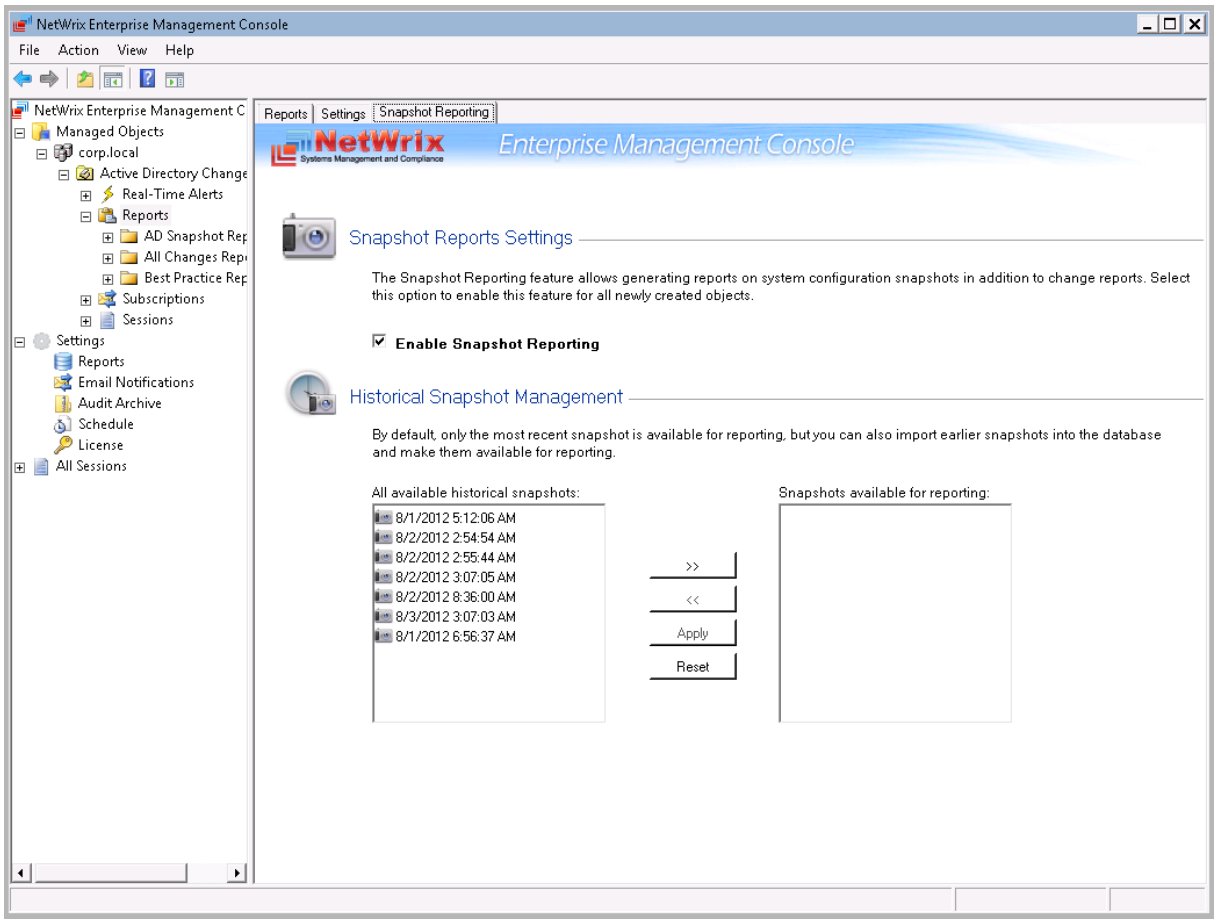
6.5.2. Importing Historical Snapshots

By default, only the most recent snapshot is available for reporting. To be able to generate reports on historical snapshots, you must import them to the database. To do this, perform the following procedure:

Procedure 20. To import historical snapshots to the SQL database

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter** → **Reports** node and select the **Snapshot Reporting** tab. The following page will be displayed:

Figure 46: Snapshot Reports Settings Page



2. Select a snapshot that you want to generate a report on from the **All available historical snapshots** list and click the >> button to add it to the **Snapshots available for reporting** list.

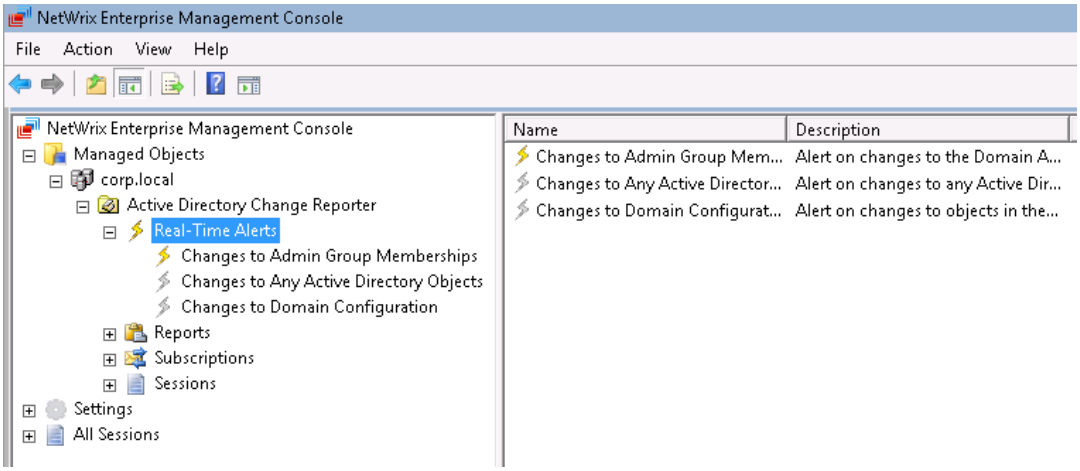
3. Repeat this step for all snapshots that you want to make available for reporting, and click the **Apply** button. Wait until connection with the Report Server is established and snapshots are imported.

7. REAL-TIME ALERTS

If you want to be notified immediately about changes to certain objects, you can configure Real-Time Alerts that will be triggered by specific events. Alerts are emailed immediately after the specified event has been detected.

To access the Real-Time Alerts feature, in NetWrix Enterprise Management Console expand the **Managed Objects → <Managed_Object_name> → Active Directory Change Reporter → Real-Time Alerts node**. A list of available alerts will be displayed in the right pane:

Figure 47: Real-Time Alerts



The following alerts have been pre-configured for your convenience:

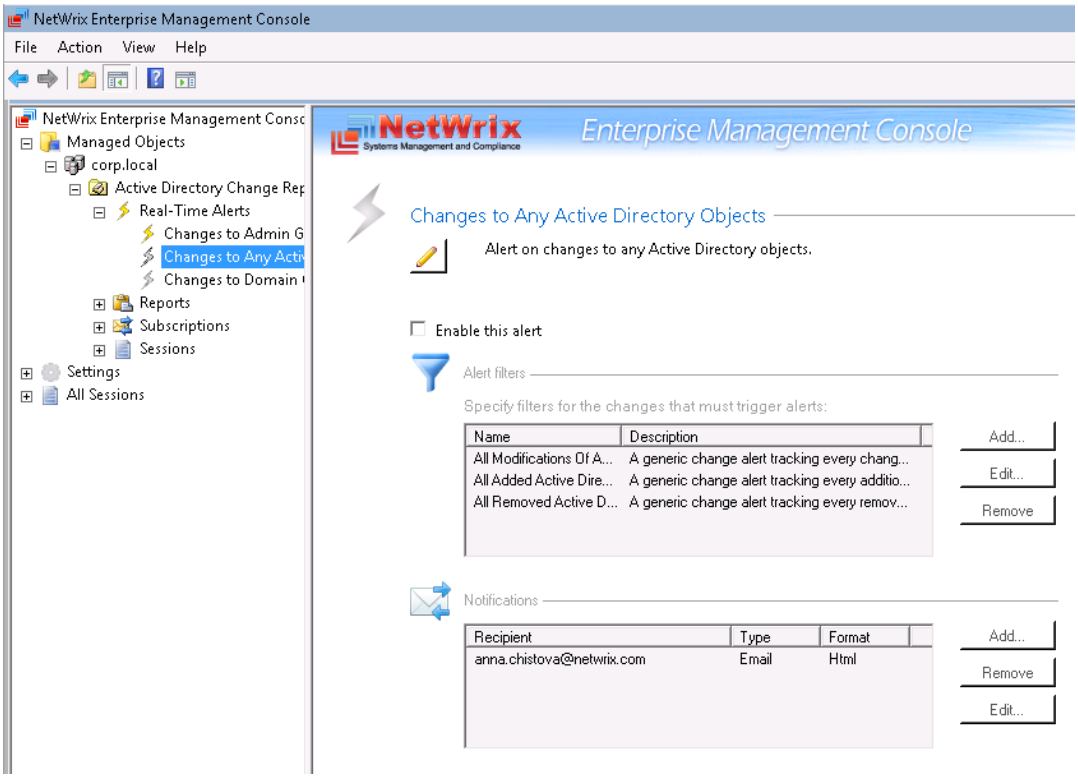
- Changes to Admin Group Membership: alerts on changes to the Domain Admins and the Enterprise Admins groups.
- Changes to Any Active Directory Objects: alerts on any changes made to any Active Directory object.
- Changes to Domain Configuration: alerts on changes to objects in domain configuration partition, such as sites, trusts, and so on.

To enable an existing alert, do the following:

Procedure 21. To enable an alert

1. Click the alerts name. Its details will be displayed in the right pane:

Figure 48: Alert Details



2. Select the **Enable this alert** option. The alert icon will turn yellow.

7.1. Creating Alerts

This section provides general instructions on how to configure Real-Time Alerts in NetWrix Active Directory Change Reporter. It also provides the algorithm for identifying the correct attribute for the type of change you want to be alerted on, which can sometimes be a difficult task if you are not sure which attribute is responsible for a specific change. For detailed instructions, refer to the following sections below:

- Configuring Real-Time Alerts
- Identifying Correct Attributes

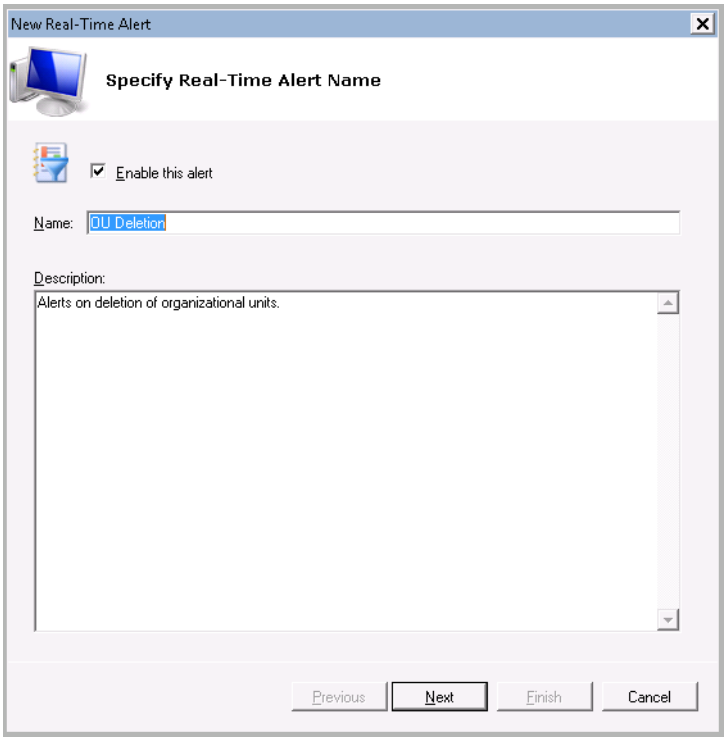
For step-by-step procedures that will guide you through configuration of some most commonly used alerts, including the "Organizational Unit Deletion" alert, the "User Account Lockout" alert and more, refer to the following NetWrix Technical Article: Configuring Real-Time Alerts in NetWrix Active Directory Change Reporter.

7.1.1. Configuring Real-Time Alerts

Procedure 22. To configure an alert

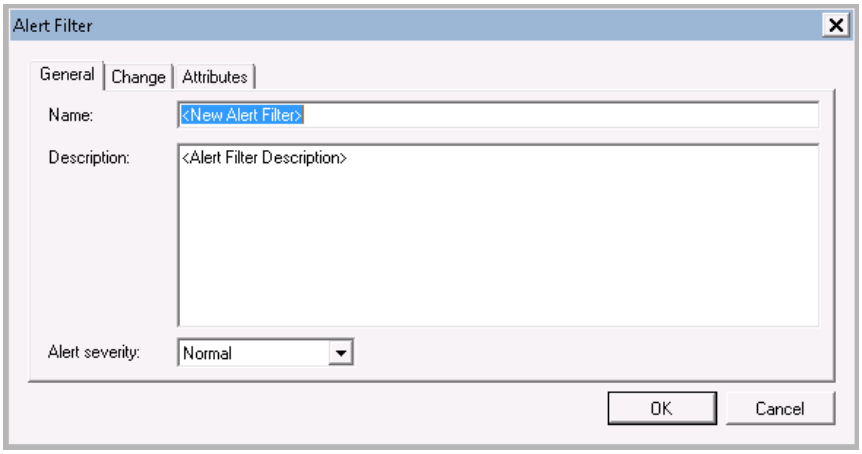
1. Right-click the Real-Time Alerts node and select **New Real-Time Change Alert** from the popup menu.
2. On the **Specify Real-Time Alert Name** step of the wizard, specify the alert name and enter alert description (optional). Click **Next** to proceed.

Figure 49: New Real-Time Alert Wizard: Specify Real-Time Alert Name



3. On the **Configure Real-Time Alert Filters and Notifications** step, you must specify alert filters and configure email notifications. Click the **Add** button in the **Alert Filters** section to specify a condition that will trigger the alert:

Figure 50: Alert Filter: General



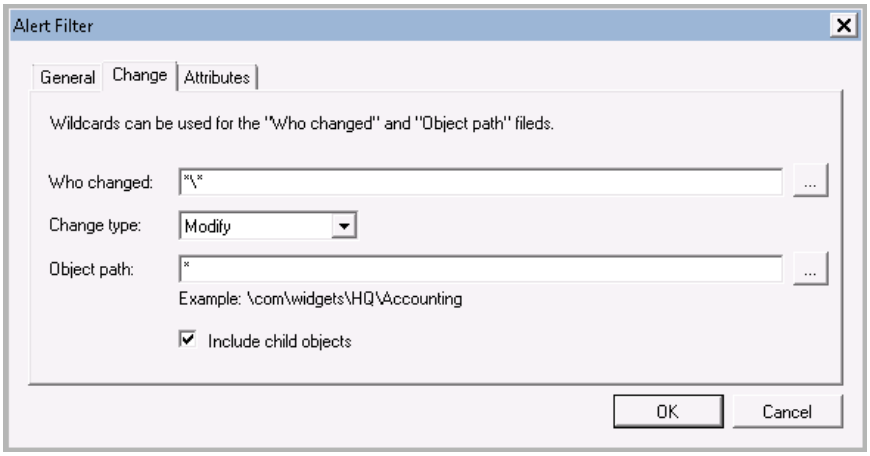
4. In the **General** tab, specify the following parameters:

Table 8: Alert Filter Parameters

Parameter	Description
Name	Specify the filter name.
Description	Enter the description for this filter (optional).
Alert severity	Select alert severity level from the drop-down list (Critical/High/Normal/Low). **NOTE**: Alert severity level will be displayed in the email notification.

5. Switch to the **Change** tab:

Figure 51: Alert Filter: Change



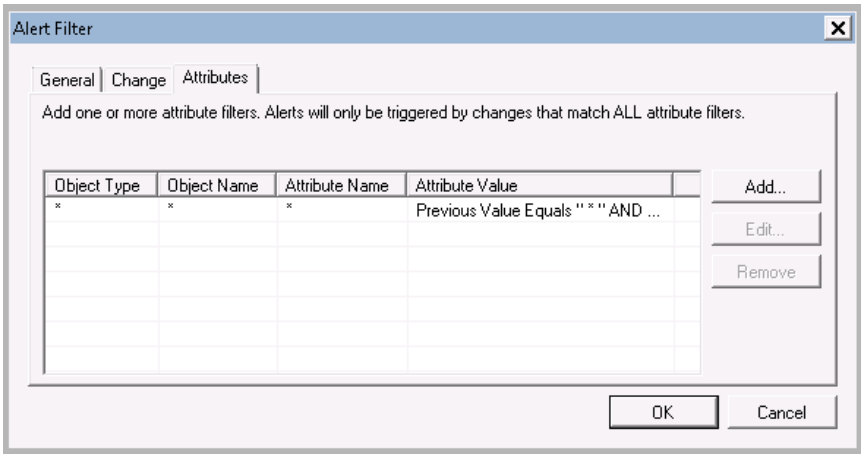
6. In the **Change** tab, specify the following filtering parameters for the alert trigger:

Table 9: Change Criterion Parameters

Parameter	Description
Who changed	Specify the name of the user whose actions must trigger the alert. You can press the ... button to select users from your domain. Alternatively, you can use a wildcard (**). In this case, the alert will be triggered if the action is performed by any user.
Change type	Select a change type (Add/Modify/Remove) from the drop-down list.
Object path	Specify the object path, i.e. the path to the AD object whose modification you want to track. You can press the ... button to browse to an AD object.
Include child objects	Select the **Include child objects** option if you want this filter to be applied to all child objects in the specified path.

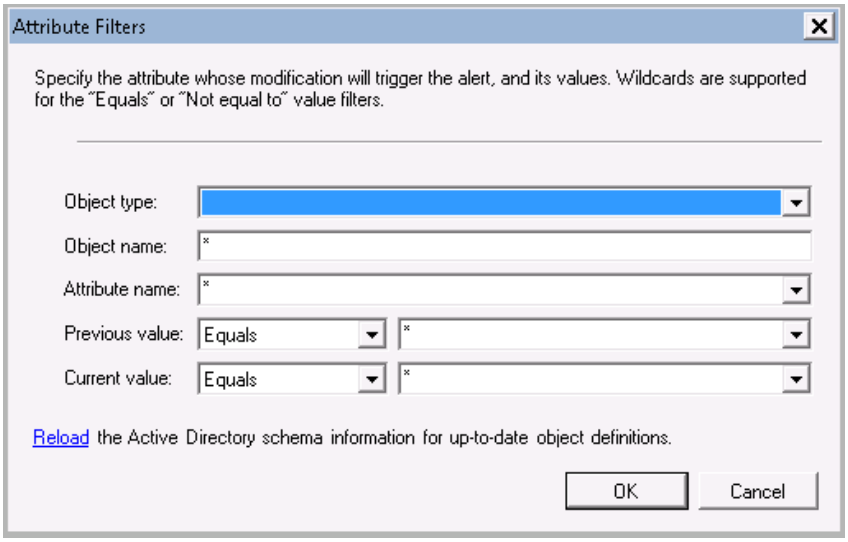
7. Switch to the **Attributes** tab:

Figure 52: Alert Filter: Attributes



8. In the **Attributes** tab you can specify an AD object attribute whose modification must trigger the alert. To do this, click the **Add** button. The **Attribute Filters** dialog will be displayed:

Figure 53: Attribute Filters



9. Specify the following parameters:

Table 10: Attribute Parameters

Parameter	Description
Object type	Select object type from the drop-down list. This list contains all Active Directory object types.
Object name	Ignore this field, as it is not used in the current Active Directory Change Reporter version.
Attribute name	From the drop-down list, select the attribute whose modification must trigger the alert. This list is populated depending on the selected object type.
Values	This field is displayed if a multi-value attribute is selected (see Figure 55: Attribute Filters: Multi-Value Attributes). Select the type of change from the drop-down list (e.g. Added or Removed), and specify the filter values.
Previous value	This field is displayed if a single-value attribute is selected (see Figure 54: Attribute Filters: Single-Value Attribute). Select a value filter from the drop-down list (possible values are: Equals, Not equal to, Starts with, Ends with, Less than, Greater than, Less or equal, Greater or equal) and specify the previous value of the attribute.
Current value	This field is displayed if a single-value attribute is selected (see Figure 54: Attribute Filters: Single-Value Attribute). Select a value filter from the drop-down list (possible values are: Equals, Not equal to, Starts with, Ends with, Less than, Greater than, Less or equal, Greater or equal) and specify the current value of the attribute.

Figure 54: Attribute Filters: Single-Value Attribute

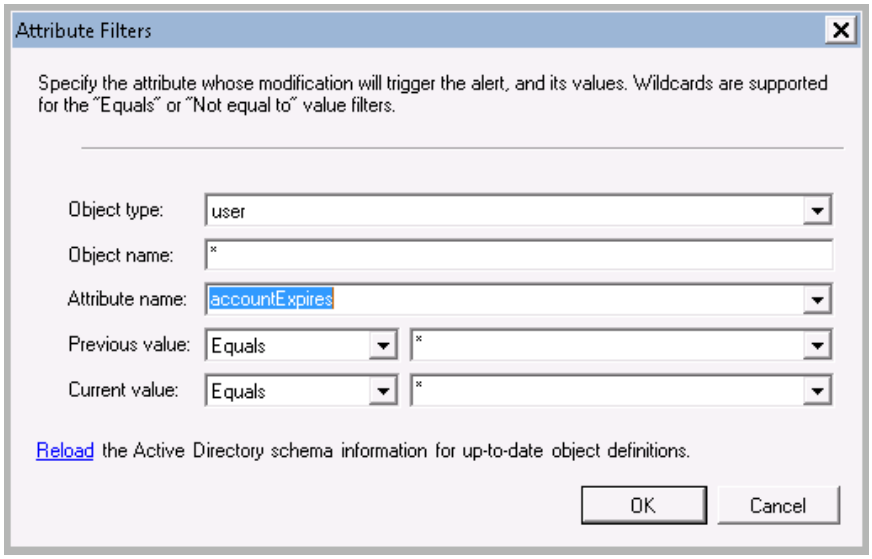
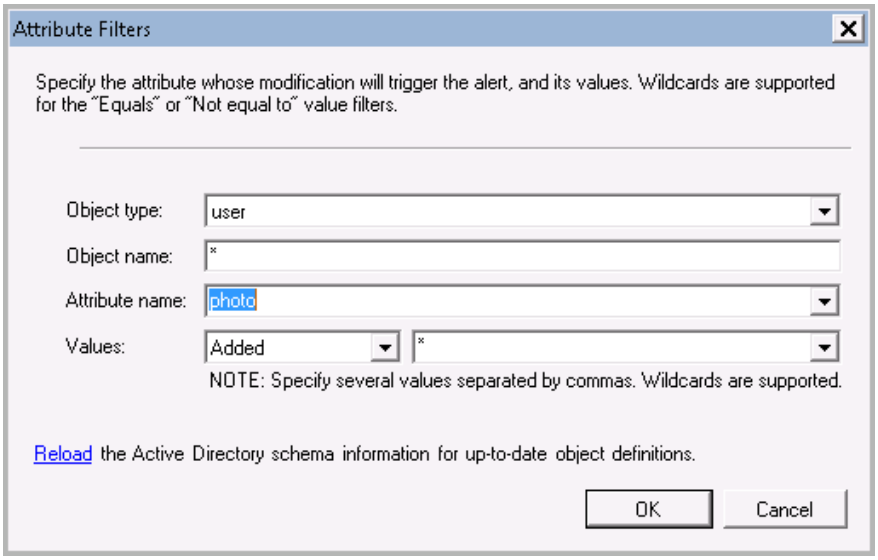


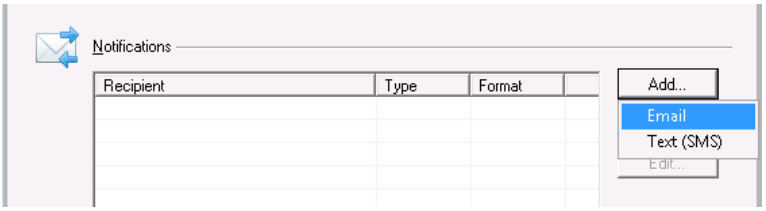
Figure 55: Attribute Filters: Multi-Value Attributes



Note: Sometimes, it can be quite difficult to select the appropriate attribute for the type of change that must trigger an alert. If you are unsure which attribute is responsible for the type of change you want to track, refer to Section 7.1.2 Identifying Correct Attributes of this guide for detailed instructions on how to identify an attribute.

10. Click **OK** to save the changes and close the **Attribute Filters** dialog.
11. In the **Notifications** section, click the **Add** button and select the **Email** option:

Figure 56: Notifications: Add Email

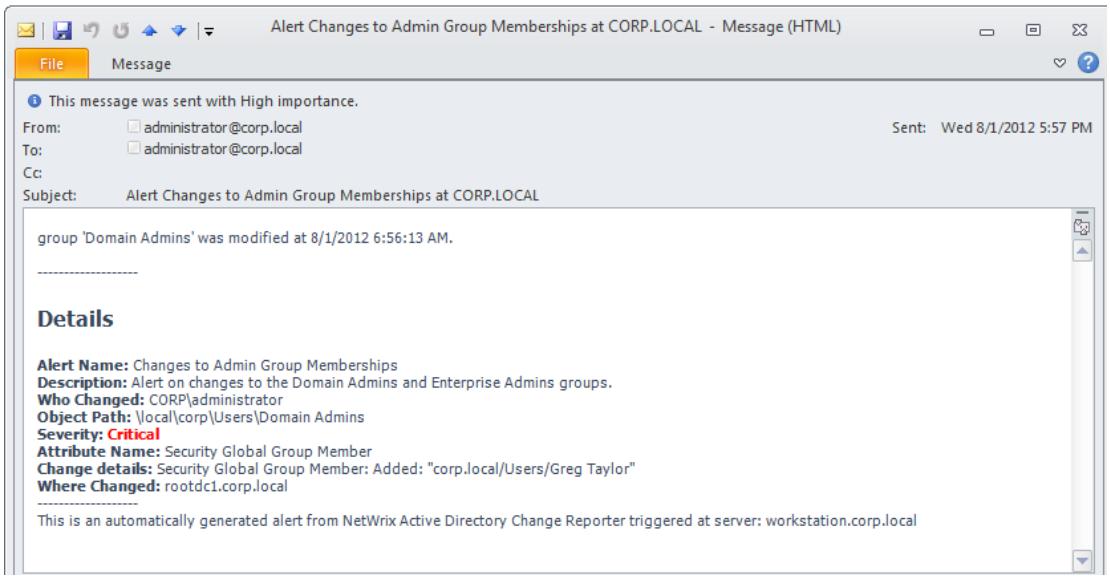


12. In the dialog that opens, specify the email address where notifications will be delivered. You can add as many recipients as necessary.

13. Click **Next** to proceed. On the last step, review your Real-Time Alert settings and click **Finish** to exit the wizard.

    The new alert will be created under the **Real-Time Alerts** node. If an event occurs that triggers an alert, an email notification like in the example below will be sent immediately to the specified recipients:

Figure 57: Real-Time Alert Example



7.1.2. Identifying Correct Attributes

To identify the attribute responsible for the type of change you want to track, do the following:

Procedure 23. To identify an attribute

1. On the domain controller, make a test change that you want to configure a Real-Time Alert for and that will act as a trigger.

2. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** and click the **Run** button in the right pane. On data collection completion, you will receive a Change Summary email containing a list of changes that have been detected.

3. In this email, look for the parameter name in the **Details** column of the corresponding change.

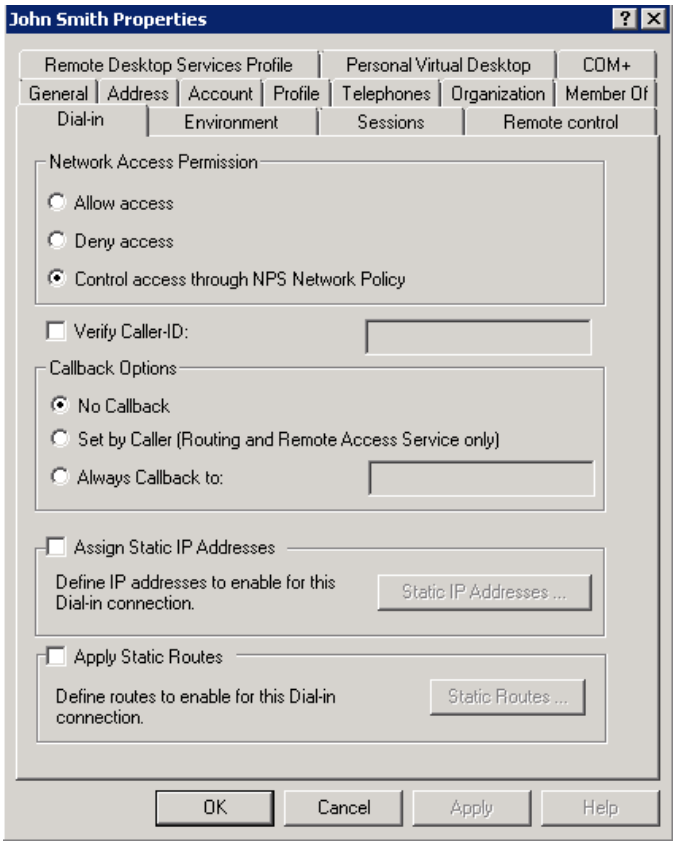
4. Open the propnames.txt file located in the product installation folder and search for this parameter name. The value corresponding to this parameter is the name of the attribute you are looking for.

Note: If you are unable to locate the parameter name in the propnames.txt file, that means that the Change Summary email contains the internal AD name for this attribute instead of a friendly name. In this case, this is the name of the attribute you are looking for that must be specified in the **Attribute Filters** dialog.

For example, if you want to create an alert that is triggered by modifications of a user's Dial-in/VPN permissions, and you are unsure which attribute is responsible for this change, do the following:

1. On the domain controller, navigate to **Start** → **Administrative Tools** → **Active Directory Users and Computers**.
2. Expand the domain node and select **Users**.
3. Right-click a user and select **Properties** from the popup menu.
4. In the user properties dialog, open the **Dial-in** tab:

Figure 58: User Properties: Dial-in Tab



5. In the **Network Access Permission** section, select the **Allow access** option and click **OK** to save the changes.
6. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** and click the **Run** button in the right pane. On data collection completion, you will receive an email containing the change you have made:

Figure 59: Change Summary

Change Type	Object Type	When Changed	Who Changed	Where Changed	Object Name	Details
Modified	user	10/7/2011 3:45:01 AM	CORP\administrator	rootdc1.corp.local	\local\corp\Users\testuser1	**Allow Dial-In** set to "TRUE"

7. In the **Details** column, locate the change parameter: Allow Dial-in.
8. Open the propnames.txt file and search for this parameter name. The entry in this file must say: `*.msNPAllowDialin=Allow Dial-In`. "msNPAllowDialin" is the name of the attribute that must be selected from the drop-down list in the **Attribute Filters** dialog when creating the alert.

8. Active Directory Object Restore

Restoring deleted objects and reverting unwanted or unauthorized changes to Active Directory objects can be a difficult and error-prone task, and sometimes it is simply impossible. In most cases, native and third-party Active Directory backup and recovery tools require non-authoritative restore and domain controllers' downtime. Moreover, they do not always have object-level restore capabilities.

With NetWrix Active Directory Change Reporter you can quickly restore deleted and modified objects using the Active Directory Object Restore tool integrated with the product. This tool enables AD object restore without rebooting a domain controller and touching the rest of the AD structure, and goes beyond the standard tombstone capabilities.

8.1. Reverting Unwanted Changes

By default, when a user or computer account is deleted from Active Directory, its password is discarded. When you restore deleted accounts with the Active Directory Object Restore tool, it sets random passwords which then have to be changed manually. If you want to be able to restore AD objects with their passwords preserved, you need to modify the Schema container settings so that account passwords are retained when accounts are deleted.

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

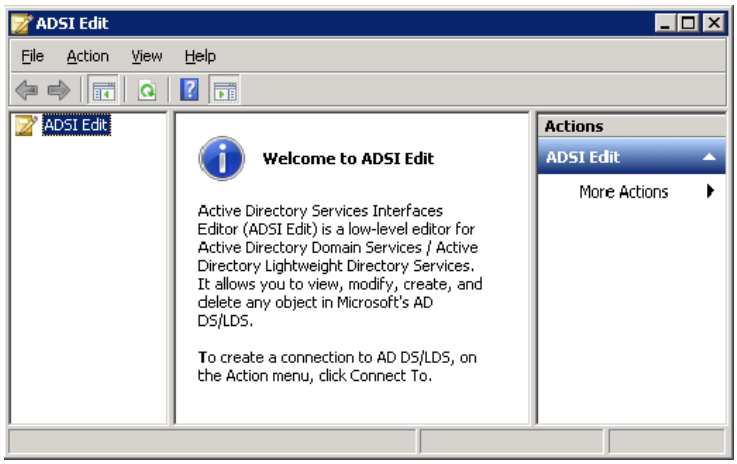
- Modify your Schema container settings to retain passwords for deleted accounts
- Revert unwanted changes to your AD objects

Procedure 24. To modify Schema container settings

Note: To perform this procedure, you will need the ADSI Edit utility. In Windows 2003 systems, this utility is a component of Windows Server Support Tools. If it has not been installed, download Windows Server Support Tools from the official website. On Windows 2008 systems and above, this component is installed together with the AD DS role.

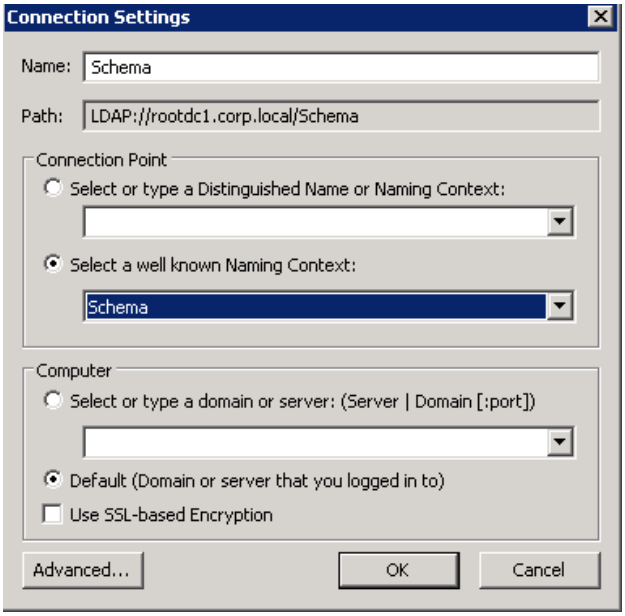
1. Navigate to **Start → Programs → Administrative Tools → ADSI Edit**. The **ADSI Edit** dialog will open.

Figure 60: ADSI Edit dialog



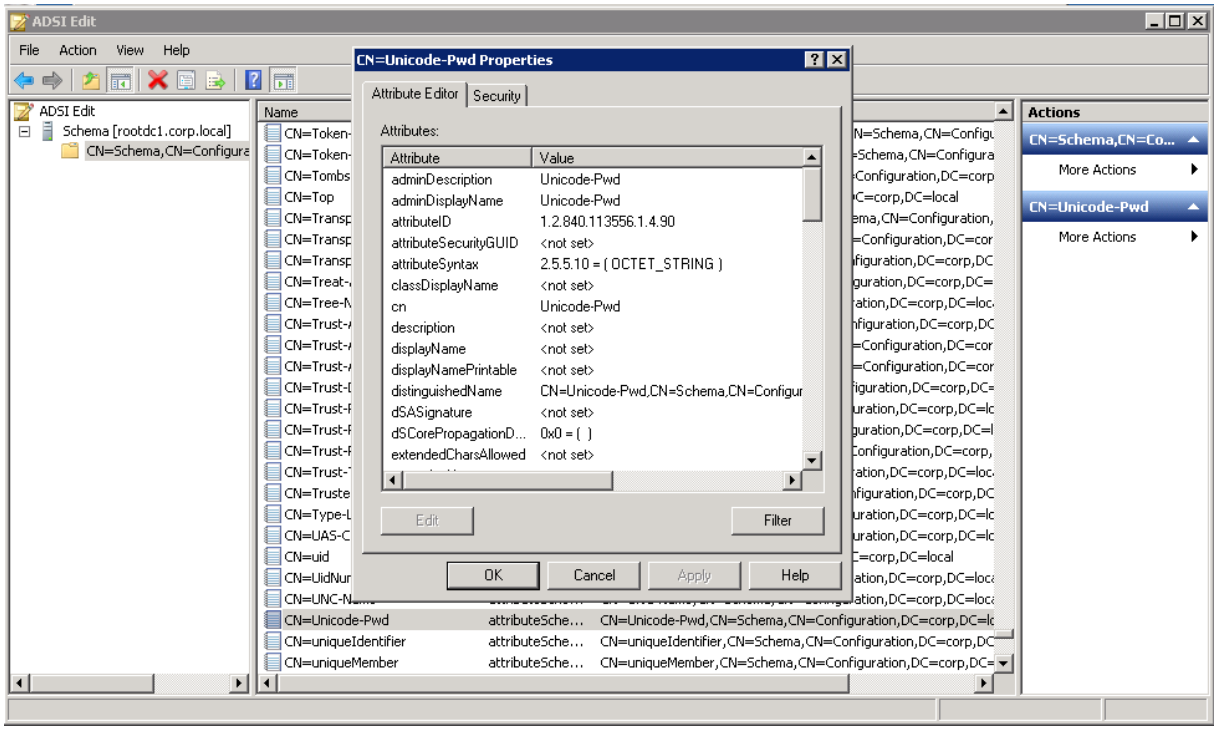
2. Right-click the **ADSI Edit** node and select the **Connect To** option. In the **Connection Settings** dialog, enable the **Select a well-known Naming Context** option and select **Schema** from the drop-down list:

Figure 61: Connection Settings Dialog



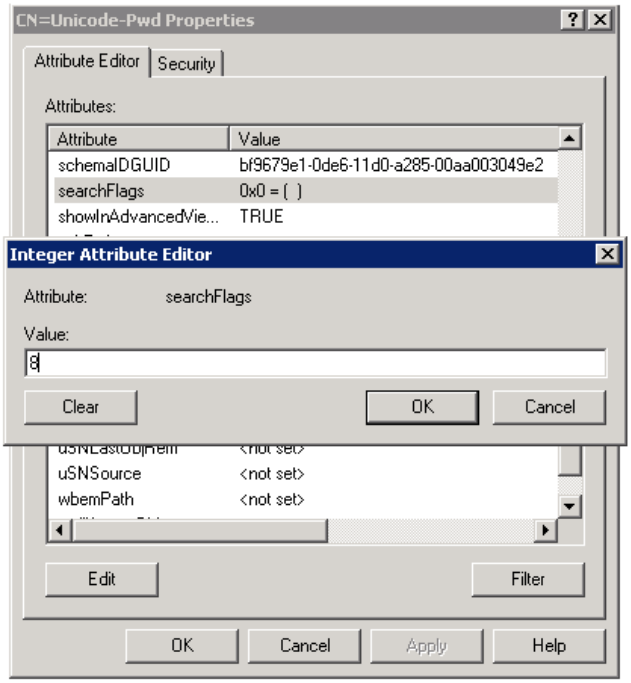
3. Click **OK**.
4. In the left pane, expand the **Schema <Your_Root_Domain_Name>** node. Locate the attribute called **CN=Unicode-Pwd**, right-click it and select **Properties** from the popup menu:

Figure 62: CN=Unicode-Pwd Properties



5. Locate the attribute called **searchFlags**, double-click it and set its value to 8:

Figure 63: Attribute Editor



6. Click **OK**.

Now you will be able to restore deleted accounts with their passwords preserved.

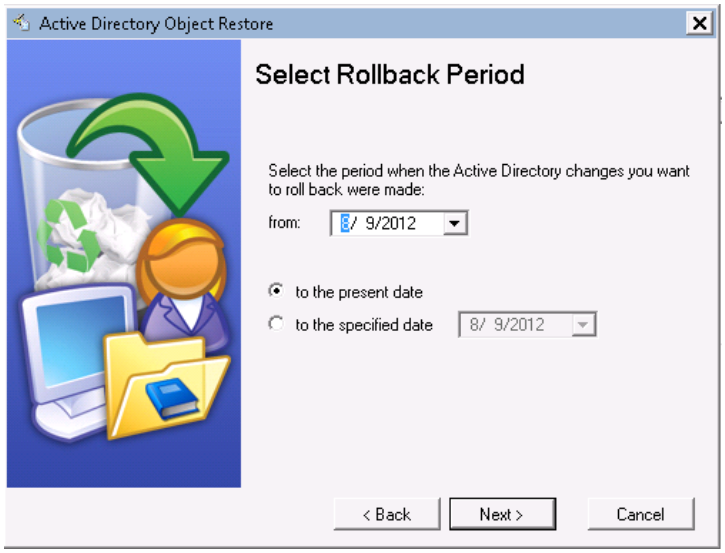
Procedure 25. To revert changes to AD objects

1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter**.
2. In the right pane, click the **Restore AD Objects** button next to **Active Directory Object Restore**. The welcome page of the Active Directory Object Restore wizard will be displayed. Click **Next** to proceed.

Figure 64: Active Directory Object Restore Wizard: Welcome Page

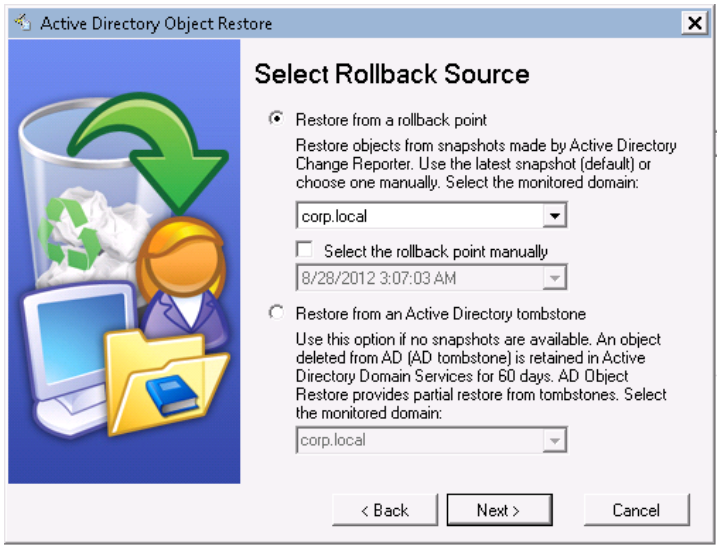
3. On the **Select Rollback Period** step, specify the period of time when unwanted changes that you want to revert occurred. You can either select a period between a specified date and the present date, or between two specified dates:

Figure 65: Active Directory Object Restore Wizard: Select Rollback Period



4. On the **Select Rollback Source** step, you must select a domain and the Rollback Source:

Figure 66: Active Directory Object Restore Wizard: Select Rollback Source



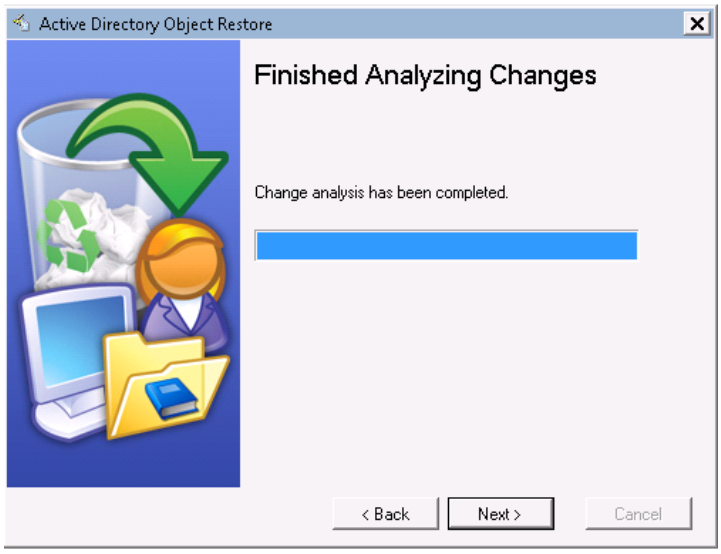
Two options are supported:

- Restore from a rollback point: this option allows restoring objects from snapshots made by NetWrix Active Directory Change Reporter. This option is more preferable since it allows attribute-level object restore.
- Restore from an Active Directory tombstone: this option is recommended when no snapshot is available. This is a last resort measure as the tombstone holds only the basic object attributes.

5. If you have selected to use a rollback point as a source, you can select the **Select the rollback point manually** option if you want to revert to a specific snapshot. Otherwise, the program will automatically search for the most recent snapshot that will cover the selected time period. Click **Next** to proceed.
6. On the **Analyzing Changes** step, the program analyzes the changes made during the specified time period. When reverting to a snapshot, the tool looks at the changes that occurred between the specified snapshots. When restoring from a tombstone,

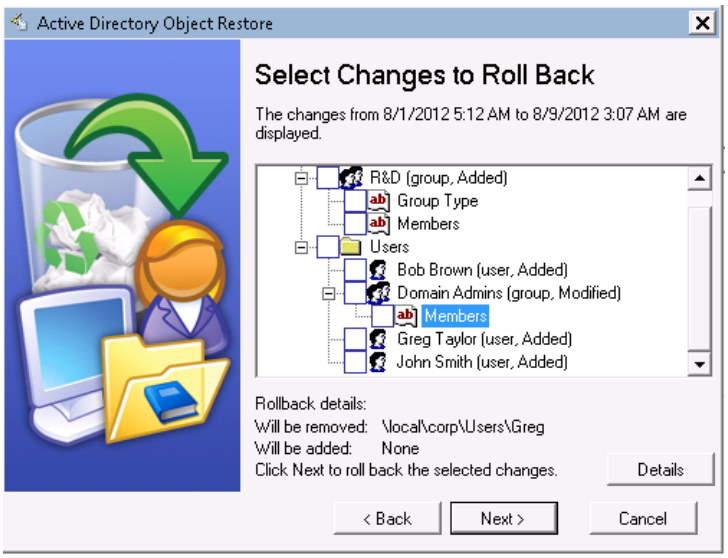
the tool looks at all AD objects put in the tombstone during the specified period of time. When the analysis is complete, click **Next** to proceed:

Figure 67: Active Directory Object Restore Wizard: Change Analysis



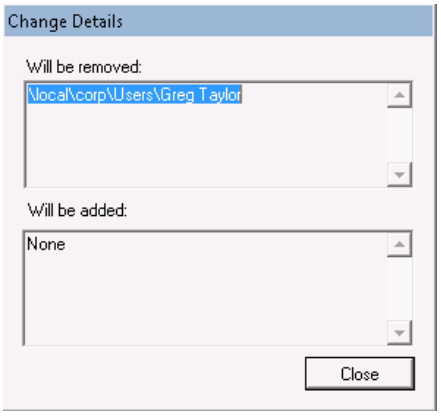
7. On the **Select Changes to Roll Back** step, the results of the analysis are displayed. Select a change to see its rollback details in the bottom of the window:

Figure 68: Active Directory Object Restore: Select Changes to Roll Back (I)



8. To see detailed rollback information on an attribute, select it and click the **Details** button. A window will popup showing what changes will be applied if this attribute is selected for rollback:

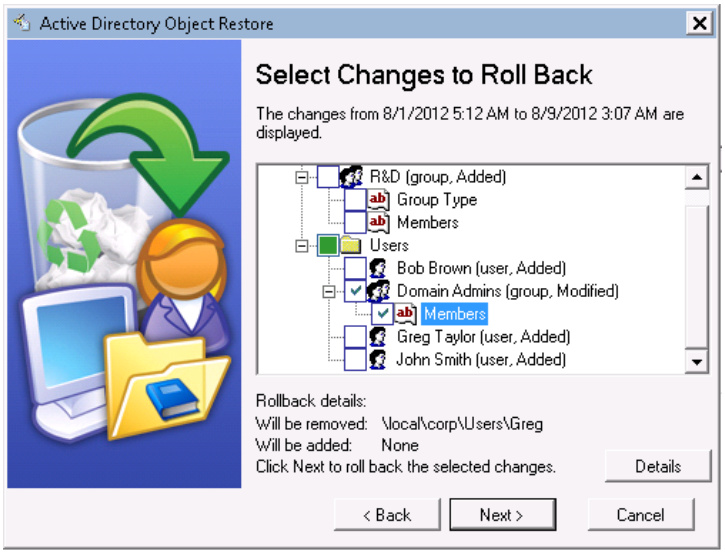
Figure 69: Change Details



9. Specify the change(s) you want to revert by selecting the corresponding check box(es) and click **Next** to restore the selected object(s) to their previous state:

Note: By default, NetWrix Active Directory Object Restore does not recover passwords and sets a random password for a restored user. The Active Directory Administrator then has to manually change a password.

Figure 70: Active Directory Object Restore Wizard: Select Changes to Roll Back (II)



10. Wait until the tool has finished restoring the selected objects. On the last step, review the results and click **Finish** to exit the wizard.

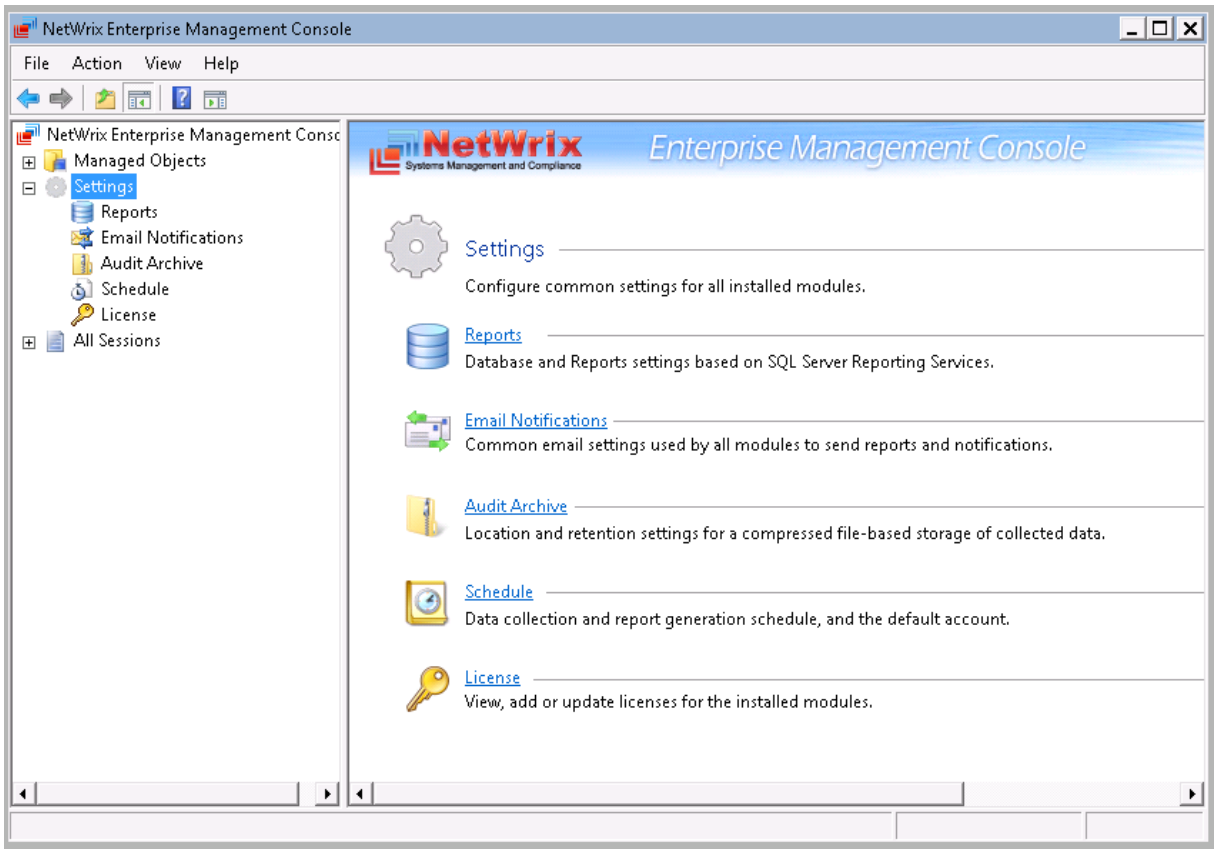
9. CONFIGURING GLOBAL SETTINGS

NetWrix Enterprise 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 71: Settings Page



The following global settings can be configured:

- Reports settings
- Email Notifications settings
- Audit Archive settings
- Default Data Processing Account
- License Settings

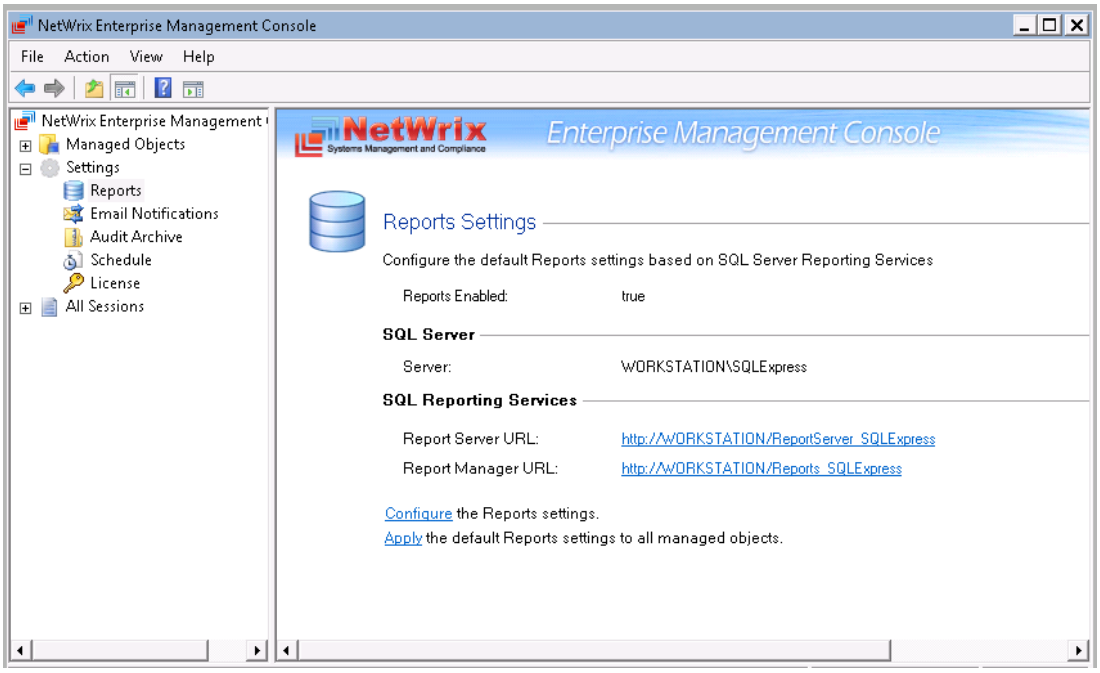
9.1. Configuring the Reports Settings

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 26. To configure the Reports settings

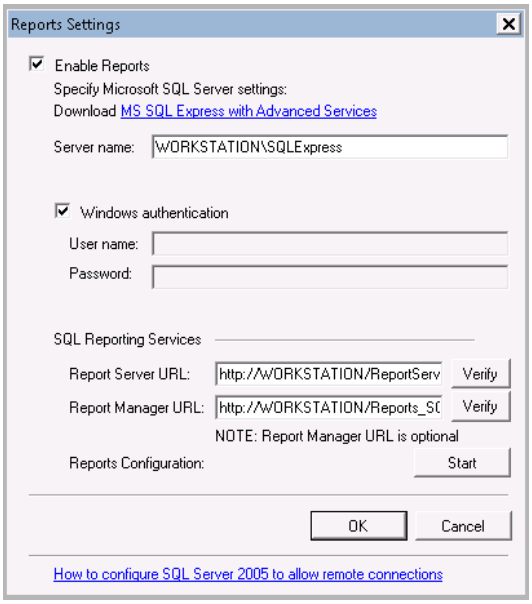
1. In NetWrix Enterprise Management Console, expand the **Settings** node and select the **Reports** node. Alternatively, you can click **Reports** in the **Settings** page. The following page will be displayed showing the current Reports settings:

Figure 72: Settings: Reports



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

Figure 73: Reports Settings



3. Specify/modify the following settings:

Table 11: Reports Settings

Parameter	Description
Enable Reports	Select this checkbox to enable the Reports feature for all Managed Objects.
Server name	Specify the name of an existing SQL Server instance where an audit

	database will be created.
Windows authentication	Select this option if you want to use the Data Processing Account you specified on Managed Object creation to access the SQL database. Deselect this option if you want to use SQL Server authentication.
User name:	Specify a user name for the SQL Server authentication. **NOTE:** This use must belong to the target Database owner role.
Password:	Specify a password for 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.
Reports Configuration	Click the **Start** button to launch the Reports Configuration wizard that automatically installs and configures Microsoft SQL Server 2005 Express with Advanced Services.

4. Click **OK** to save your changes and then **Yes** in the confirmation message to apply these settings to all Managed Objects.

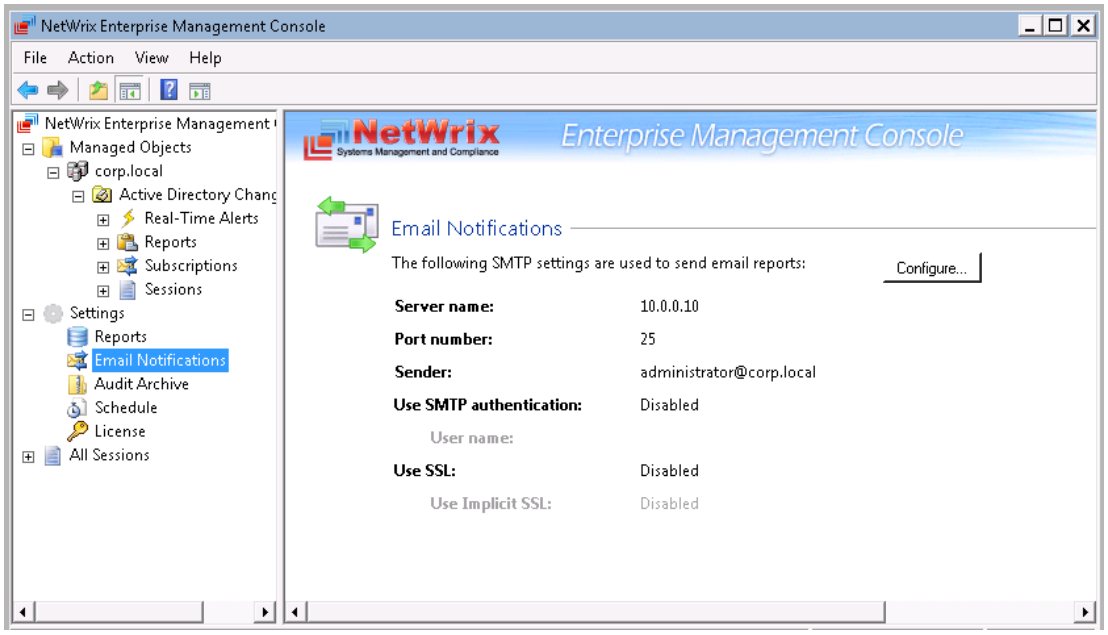
9.2. Configuring the Email Notifications Settings

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 27. To configure the email notifications settings

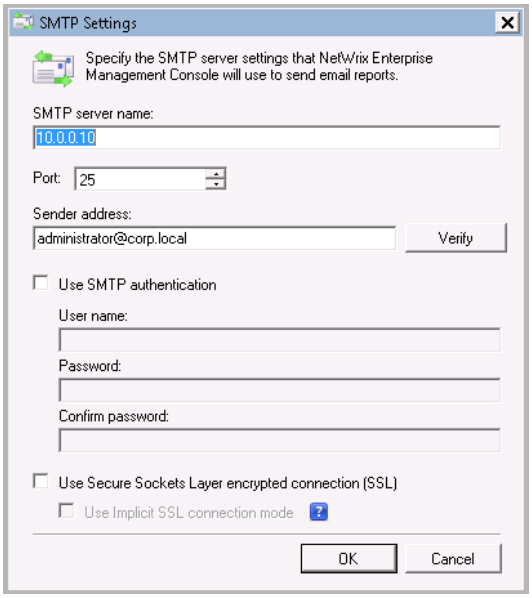
1. In NetWrix Enterprise Management Console, expand the **Settings** node and select the **Email Notifications**. Alternatively, you can click **Email Notifications** in the Settings page. The following page will be displayed showing the current email settings:

Figure 74: Settings: Email Notifications



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

Figure 75: 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.

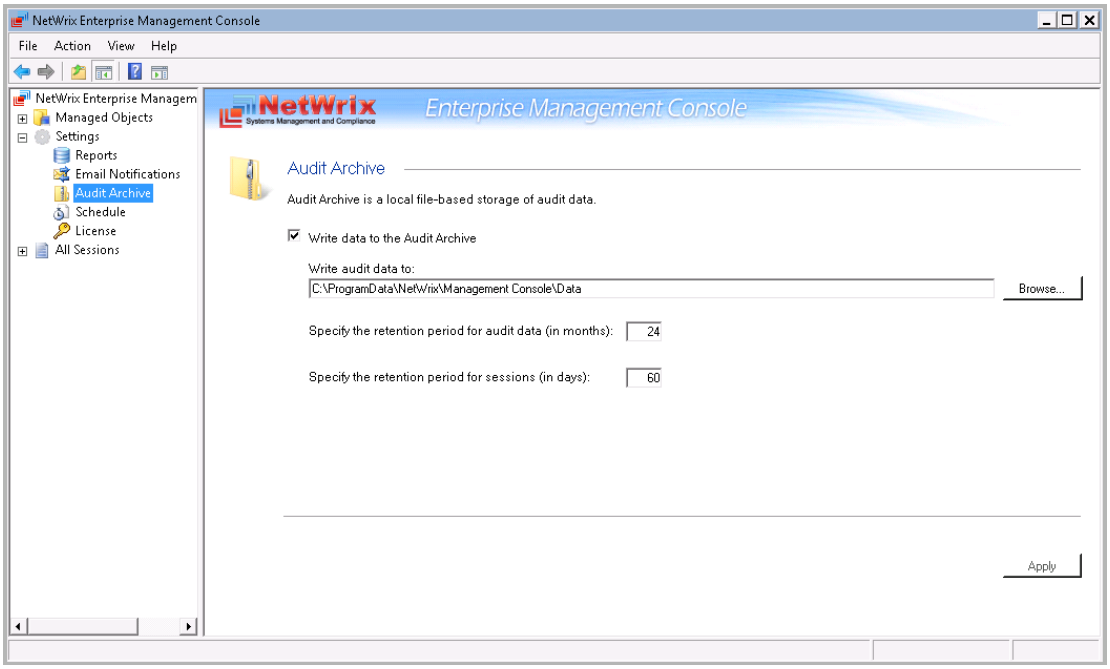
9.3. Configuring Audit Archive Settings

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

Procedure 28. To configure the Audit Archive settings

1. In NetWrix Enterprise 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 76: Settings: Audit Archive



2. Modify the following settings if necessary:

Table 12: Audit Archive Settings

Parameter	Description
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	Specify the number of months for which audit data will be stored. Data will be deleted automatically when its retention period is over.
Specify the retention period for sessions	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 Enterprise 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.

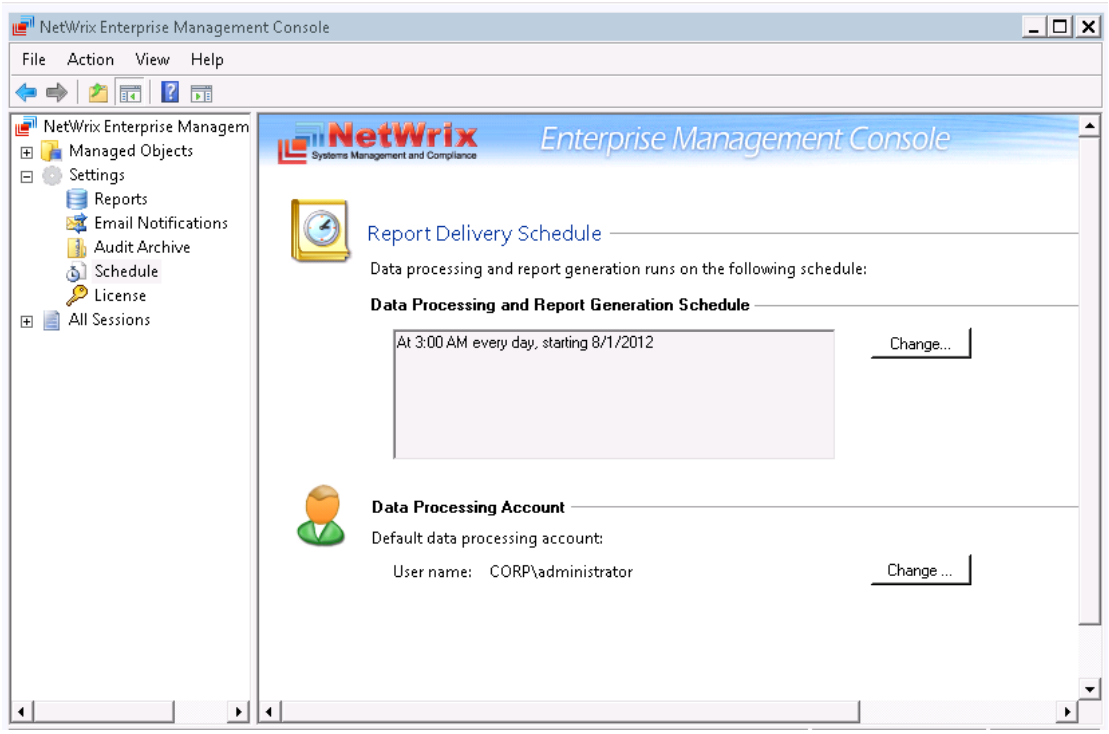
9.4. Configuring Default Data Processing Account

The **Schedule** option allows modifying the default Data Processing Account.

Procedure 29. To modify the default Data Processing Account

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

Figure 77: Settings: Schedule



2. Click the **Change** button next to **Default data processing account**. In the dialog that opens, specify the account and its credentials and click **OK**.

Note: The **Data Processing and Report Generation Schedule** option is inapplicable to NetWrix Active Directory Change Reporter, as it has its own scheduled task. For instructions on how to modify the Change Summary generation schedule for NetWrix Active Directory Change Reporter, refer to Procedure 4 To modify Active Directory Change Reporter settings.

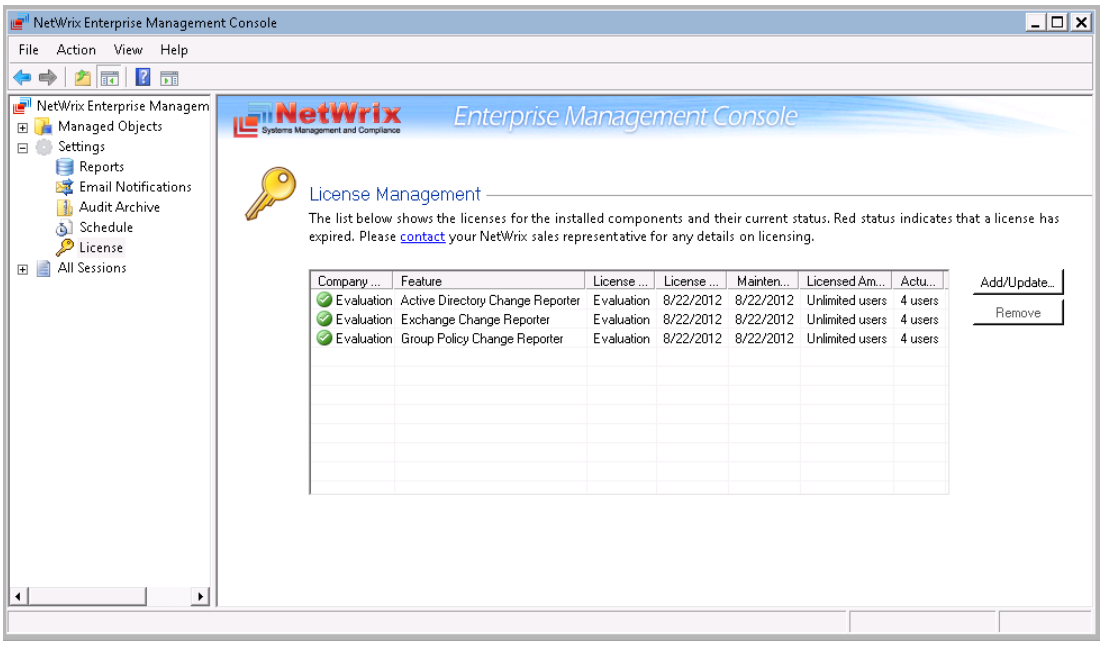
9.5. Configuring License Settings

The **License** 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 30. To configure licenses

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

Figure 78: Settings: License



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 install multiple licenses at the same time if they have the same license count. Otherwise, install them separately.

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

   Note: NetWrix Active Directory Change Reporter is part of a larger change reporter pack that includes the following three modules:

   - NetWrix Active Directory Change Reporter
   - NetWrix Exchange Change Reporter
   - NetWrix Group Policy Change Reporter

Licenses for each of these modules have to be purchased separately. When you install the Enterprise Edition without purchasing a license, you can use the product forming the pack free of charge for 20 days. If you then purchase a license for one of the modules, the other modules will switch to the Freeware mode.

10. ADDITIONAL CONFIGURATION

This Chapter provides instructions on how to fine-tune NetWrix Active Directory Change Reporter using the additional configuration options. It explains how to:

- Enable monitoring of the Configuration and Schema partitions
- Enable integration with third-party SIEM solutions, including Microsoft System Center Operations Manager (SCOM)
- Exclude or include certain data types from/in reports

10.1. Enabling Monitoring of AD Partitions

In an Active Directory environment, every domain controller contains the following three directory partitions:

- **Configuration partition**: stores configuration objects for the entire forest. Updates to this partition are replicated to all domain controllers in the forest. Configuration objects store the information on sites, services, and directory partitions.
- **Schema partition**: stores class and attribute definitions for all existing and possible Active Directory objects. Updates to this partition are replicated to all domain controllers in the forest.
- **Domain partition**: stores users, computers, groups and other objects. Updates to this partition are replicated only to domain controllers within the domain.

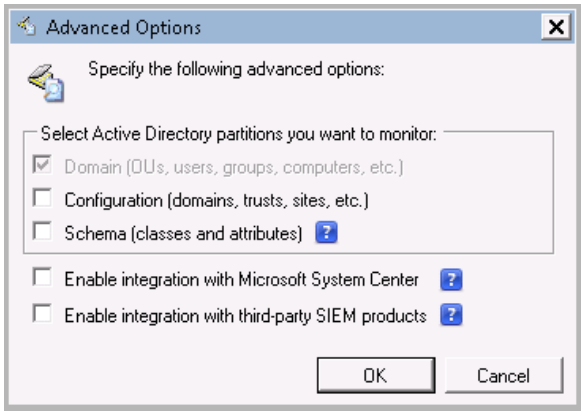
By default, NetWrix Active Directory Change Reporter only monitors changes to the Domain partition and the Configuration partition of the monitored domain. If you also want to monitor changes to the Schema partition, or to disable monitoring of changes to the Configuration partition do the following:

Note: You cannot disable monitoring of changes to the Domain partition.

Procedure 31. Enabling monitoring of the Configuration and Schema partitions

1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter**.
2. In the right pane, click the **Configure** button next to **Advanced Options**. The following dialog will be displayed:

Figure 79: Advanced Options Dialog



3. Enable the **Configuration** and/or **Schema** options and click **OK** to save the changes.

Information on changes to the selected partition(s) will be available in Reports and will be saved in snapshots.

10.2. Enabling Integration with Third-Party SIEM Solutions

If your organization is already using a third-party Security Information and Event Management (SIEM) solution, NetWrix Active Directory Change Reporter can help protect these investments by integrating with major SIEM systems and letting you manage audit data in your usual way, but with improved performance and increased reliability of collected audit data.

NetWrix Active Directory Change Reporter can integrate with all major SIEM solutions, including Microsoft SCOM, RSA enVision®, ArcSight® Logger™, Novell® Sentinel™, NetIQ® Security Manager™, IBM Tivoli® Security Information and Event Manager™, and many others.

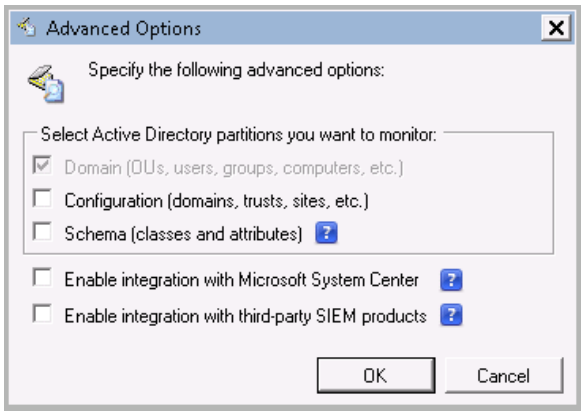
If integration with SIEM products is enabled, a custom Windows event log is created called NetWrix Change Reporter. This event log will generate events for each detected change (for detailed information on such events and their IDs, refer to the following NetWrix Technical Article: Integration with Third Party SIEM Systems). You can configure custom processing rules, alerts and reports in your SIEM solution to react to these events.

If you are using Microsoft System Center Operations Manager (SCOM) and want to integrate it with NetWrix Active Directory Change Reporter, you need to install NetWrix Active Directory Change Reporter SCOM Management Pack, which is a solution that captures events written by NetWrix Active Directory Change Reporter into the dedicated event log, and then feeds it to Microsoft SCOM that generates corresponding reports and alerts (for a detailed description of alerts triggered by SCOM alerting rules, refer to the following NetWrix Technical Article: NetWrix Active Directory Change Reporter SCOM Alerts Specification).

Procedure 32. To enable integration with third-party SIEM solutions

1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** → **Active Directory Change Reporter**.
2. In the right pane, click the **Configure** button next to **Advanced Options**. The following dialog will be displayed:

Figure 80: Advanced Options Dialog



3. Select the **Enable integration with Microsoft System Center** option to integrate the product with Microsoft SCOM, or the **Enable integration with third-party SIEM products** option to integrate the product with a different SIEM solution, and click **OK** to save the changes.

10.3. Excluding/Including Data Types from/in Reports

You can fine-tune NetWrix Active Directory Change Reporter by specifying various data types that you want to exclude from product reports. 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, their descriptions, syntax and examples. One entry per line is accepted.

Table 13: NetWrix Active Directory Change Reporter Configuration Files

File Name	Description	Syntax	Example
addprops.txt	Allows adding properties to appear in the Change Summaries for newly created AD objects. When a new object is added, NetWrix Active Directory Change Reporter does not show any data in the Details column in the Change Summary emails. If you want to see the information on certain attributes of a newly created object, specify these attributes in this file.	<object type>:<property>:	To show a group description on this group's creation, add the following line: `group:description:`
allowedpathlist.txt	Contains a list of AD paths to be included in change reports. This file can be used, for example, if you only want to monitor specific OU(s) inside your AD domain, and not the entire domain. In this case, put a wildcard (*) in the omitpathlist.txt file to exclude all paths, and then specify the OU(s) you want to monitor in the allowedpathlist.txt file.	<path> The path must be in the format displayed in the Object Name column in the Change Summary or the What Changed column in SSRS-based Reports. **NOTE**: A wildcard (*) can be used to replace any number of characters.	To monitor only the Users OU in domain CORP, add the following line: `\local\corp\Users\*` In the omitpathlist.txt file, specify the wildcard (*)

omitallowedpathlist.txt	Contains a list of AD paths to be excluded from Change Summaries and Reports. This file can be used if you want to exclude certain paths inside those specified in the allowedpathlist.txt file. In this case, put a wildcard (*) in the omitpathlist.txt file to exclude all paths, then specify the OU(s) you want to monitor in the allowedpathlist.txt file, and then specify the paths you want to exclude from within them in the omitallowedpathlist.txt file.	<path>
		The path must be in the format displayed in the Object Name column in the Change Summary or the What Changed column in SSRS-based Reports.
		NOTE: A wildcard (*) can be used to replace any number of symbols.
			To monitor the Users OU, but to exclude users jsmith and pbrown from it, do the following:
			• Add the wildcard (*) to the omitpathlist.txt file.
			• Add the following line to the allowedpathlist.txt file:
			`*\Users\*`
			• Add the following lines to the omitallowedpathlist.txt file:
			`*\jsmith`
			`*\pbrown`

omitobjlist.txt	Contains a list of object types to be excluded from change reports.	<object type> **NOTE**: A wildcard (*) can be used instead of an object type if you want to exclude all	To omit changes to the printQueue object, add the following line: `printQueue`

File Name	Description	Syntax	Example
		object types.	
omitpathlist.txt	Contains a list of AD paths to be excluded from change reports.	<path> The path must be in the format displayed in the Object Name column in the Change Summary or the What Changed column in SSRS-based Reports. **NOTE**: A wildcard (*) can be used to replace any number of symbols.	To exclude changes to the Service Desk OU, add the following line: `*\Service Desk\*`
omitproplist.txt	Contains a list of object types and properties to be excluded from change reports.	<object type>.<property> **NOTE**: A wildcard (*) can be used instead of an object type or a property name to exclude all object types/property names. If there is no separator (.) between an object type and a property name, the whole entry is treated as an object type.	To exclude the adminCount property from Reports, add the following line: `*.adminCount`
omitreporterrors.txt	Contains a list of errors to be excluded from Change Summaries.	<errorname> **NOTE**: A wildcard (*) can be used for an error name if you want to exclude all errors.	If you have granular audit settings applied to your domain controllers policy, the following error will be returned in the Change Summary emails: `Auditing of Directory Service Access is not enabled for this DC. Adjust the audit policy settings using the Active Directory Audit Configuration Wizard or see the product documentation for more information.` Add the text of this error message to this file to stop getting it in the Change Summary emails.
omitsnapshotpathlist.txt	Contains a list of AD paths to be excluded from AD snapshots.	<path> The path must be in the format displayed in the Object Name column in the Change Summary or the What Changed column in SSRS-based Reports. **NOTE**: A wildcard (*) can be used to replace	To exclude data on the Disabled Accounts OU from Snapshot Report, add the following line: `*\Disabled Accounts*`

File Name	Description	Syntax	Example
		any number of symbols.	
omitstorelist.txt	Contains a list of object types and properties to be excluded from AD snapshots.	<object type>.<property> **NOTE**: A wildcard (*) can be used instead of an object type or a property name to exclude all object types/property names. If there is no separator (.) between an object type and a property name, the whole entry is treated as an object type.	To exclude data on the AD property adminDescription, add the following line: `*.adminDescription`
processaddedprops.txt	Allows adding properties to appear in change reports (SSRS-based) for newly created AD objects. When a new object is created, NetWrix Active Directory Change Reporter does not show any data in the Details column in reports. If you want to see the information on certain attributes of a newly created object, specify these attributes in this file.	<object>:<property>:	If you want a user's Description property to be displayed in Reports when a user is added, add the following line: `User:Description:`
processdeletedprops.txt	Allows adding properties to appear in change reports (SSRS-based) for deleted AD objects. When an object is deleted, NetWrix Active Directory Change Reporter does not show any data in the Details column in reports. If you want to see the information on certain attributes of a deleted object, specify these attributes in this file.	<object>:<property>:	If you want a user's Description property to be displayed in Reports when a user is deleted, add the following line: `User:Description:`
propnames.txt	Contains a list of human-readable names for object types and properties to be displayed in change reports.	<object type>.<property>=<intelligible name>	If you want the adminDescription property to be displayed in reports as Admin Screen Description, add the following line: `*.adminDesciption=Admin Screen Description`

A APPENDIX: MONITORED OBJECT TYPES AND ATTRIBUTES

NetWrix Active Directory Change Reporter tracks changes made to all object classes and attributes in the Active Directory Domain, Configuration and Schema partitions. It also tracks changes to new object classes and attributes added due to the Active Directory Schema extension.

See a list of all Active Directory object classes

See a list of all Active Directory object attributes

B APPENDIX: SQL DATABASE RETENTION SCRIPT

```
DECLARE @Retention_Period_Days int
SET @Retention_Period_Days = 90 --Please specify the retention period in days (1 or more).
/*****************************************************************************************/
DECLARE @DB sysname
SET @DB = DB_NAME()
exec sp_executesql N'
USE [msdb];

IF  EXISTS (SELECT job_id FROM msdb.dbo.sysjobs_view WHERE name = N''Retention Job'')
BEGIN
          declare @j_id uniqueidentifier
          SELECT @j_id=job_id FROM msdb.dbo.sysjobs_view WHERE name = N''Retention Job''
          EXEC msdb.dbo.sp_delete_job @job_id=@j_id, @delete_unused_schedule=1
END;

USE [msdb];

BEGIN TRANSACTION
DECLARE @ReturnCode INT
SELECT @ReturnCode = 0

IF NOT EXISTS (SELECT name FROM msdb.dbo.syscategories WHERE name=N''[Uncategorized
(Local)]'' AND category_class=1)
BEGIN
EXEC @ReturnCode = msdb.dbo.sp_add_category @class=N''JOB'', @type=N''LOCAL'',
@name=N''[Uncategorized (Local)]''
IF (@@ERROR <> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback

END

DECLARE @jobId BINARY(16)
DECLARE @desc nvarchar(100)
SET @desc = N''A scheduled job that deletes all data that is older than ''+CAST(@Retention As
nvarchar(100))+'' day(s).''
EXEC @ReturnCode =  msdb.dbo.sp_add_job @job_name=N''Retention Job'',
                    @enabled=1,
                    @notify_level_eventlog=0,
                    @notify_level_email=0,
                    @notify_level_netsend=0,
                    @notify_level_page=0,
                    @delete_level=0,
                    @description=@desc,
                    @category_name=N''[Uncategorized (Local)]'',
                    @owner_login_name=N''sa'', @job_id = @jobId OUTPUT
IF (@@ERROR <> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback

DECLARE @sqlcommand nvarchar(max)

SET @sqlcommand = N''
DECLARE @RetDays int
DECLARE @Date datetime

Set @RetDays = ''+CAST(@Retention As nvarchar(100))+''
Set @Date = DATEADD(d, -1*@RetDays, GETUTCDATE())

IF EXISTS (select * from [dbo].[DBVersion] where ProductId = 0 AND DBVersion = 4)
BEGIN
          BEGIN TRAN

          IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N''''[dbo].[GPOPropChanges]'''') AND type in (N''''U''''))
          Delete gpc
          From
                    GPOPropChanges gpc
                    inner join GPOFolderChanges gfc on gpc.GPOFolderId = gfc.GPOFolderChangeId
                    inner join Changes c on gfc.ChangeId = c.ChangeId
                    inner join Sessions s on c.ProductId = s.ProductId and c.SessionId =
s.SessionId
          Where
                    s.Date < @Date
          If (@@ERROR>0) GOTO QuitWithRollback

          IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N''''[dbo].[GPOFolderChanges]'''') AND type in (N''''U''''))
          Delete gfc
```

```
          From
                    GPOFolderChanges gfc
                    inner join Changes c on gfc.ChangeId = c.ChangeId
                    inner join Sessions s on c.ProductId = s.ProductId and c.SessionId =
s.SessionId
          Where
                    s.Date < @Date
          If (@@ERROR>0) GOTO QuitWithRollback

          IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N''''[dbo].[PropChanges]'''') AND type in (N''''U''''))
          Delete pc
          From
                    PropChanges pc
                    inner join Changes c on pc.ChangeId = c.ChangeId
                    inner join Sessions s on c.ProductId = s.ProductId and c.SessionId =
s.SessionId
          Where
                    s.Date < @Date
          If (@@ERROR>0) GOTO QuitWithRollback

          IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N''''[dbo].[ObjProps]'''') AND type in (N''''U''''))
          Delete op
          From
                    ObjProps op
                    inner join Changes c on op.ChangeId = c.ChangeId
                    inner join Sessions s on c.ProductId = s.ProductId and c.SessionId =
s.SessionId
          Where
                    s.Date < @Date
          If (@@ERROR>0) GOTO QuitWithRollback

          IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N''''[dbo].[Changes]'''') AND type in (N''''U''''))
          Delete c
          From
                    Changes c
                    inner join Sessions s on c.ProductId = s.ProductId and c.SessionId =
s.SessionId
          Where
                    s.Date < @Date
          If (@@ERROR>0) GOTO QuitWithRollback

          IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N''''[dbo].[Sessions]'''') AND type in (N''''U''''))
          Delete s
          From
                    Sessions s
          Where
                    s.Date < @Date
          If (@@ERROR>0) GOTO QuitWithRollback

          COMMIT TRANSACTION
          GOTO EndSave
          QuitWithRollback:
                    IF (@@TRANCOUNT > 0) ROLLBACK TRANSACTION
          EndSave:
END

IF EXISTS (select * from [dbo].[DBVersion] where ProductId = 0 AND DBVersion >= 5)
BEGIN
          exec sp_netwrix_DatabaseMaintenance @Date, 0
END
                    ''
EXEC @ReturnCode = msdb.dbo.sp_add_jobstep @job_id=@jobId, @step_name=N''Retention Step'',
                    @step_id=1,
                    @cmdexec_success_code=0,
                    @on_success_action=1,
                    @on_success_step_id=0,
                    @on_fail_action=2,
                    @on_fail_step_id=0,
                    @retry_attempts=0,
                    @retry_interval=0,
                    @os_run_priority=0, @subsystem=N''TSQL'',
                    @command=@sqlcommand,
                    @database_name=@DBName,
                    @flags=0
IF (@@ERROR <> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback
```

```
EXEC @ReturnCode = msdb.dbo.sp_update_job @job_id = @jobId, @start_step_id = 1
DECLARE @scheduleId uniqueidentifier
IF (@@ERROR <> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback
EXEC @ReturnCode = msdb.dbo.sp_add_jobschedule @job_id=@jobId, @name=N''Retention Schedule'',
                   @enabled=1,
                   @freq_type=4,
                   @freq_interval=1,
                   @freq_subday_type=1,
                   @freq_subday_interval=0,
                   @freq_relative_interval=0,
                   @freq_recurrence_factor=0,
                   @active_start_date=NULL,
                   @active_end_date=99991231,
                   @active_start_time=20000,
                   @active_end_time=235959
IF (@@ERROR <> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback
EXEC @ReturnCode = msdb.dbo.sp_add_jobserver @job_id = @jobId, @server_name = N''(local)''
IF (@@ERROR <> 0 OR @ReturnCode <> 0) GOTO QuitWithRollback
COMMIT TRANSACTION
GOTO EndSave
QuitWithRollback:
    IF (@@TRANCOUNT > 0) ROLLBACK TRANSACTION
EndSave:
',
N'@DBName sysname, @Retention int', @DBName = @DB, @Retention = @Retention_Period_Days
```

C APPENDIX: NETWRIX ACTIVE DIRECTORY CHANGE REPORTER REGISTRY KEYS

The table below contains the description of the NetWrix Active Directory Change Reporter registry keys that you may need to configure while using the product. To configure/modify a registry key, navigate to **Start → Run**, and type `regedit` to launch Registry Editor.

Table 14: NetWrix Active Directory Change Reporter Registry Keys

Registry Key	Type	Description/Values	Created on installation	Preserved during upgrade
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432NODE)\NetWrix\AD Change Reporter\<Managed Object name>\ Database Settings				
SessionIncrementalUpdate	REG_DWORD	Defines whether to perform incremental update for database statistics on each data collection. 0 – no 1 - yes	No **Note:** This key is created automatically if the Snapshot Reporting feature is enabled for this Managed Object	No
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\NetWrix\AD Change Reporter				
CleanAutoBackupLogs	REG_DWORD	Defines the retention period for the security log backups: 0 – backups are never deleted from DCs [x] – backups are deleted after [x] hours	Yes	Yes
IgnoreAuditCheckResultError	REG_DWORD	Defines whether audit check errors should be displayed in the Change Summary footer: 0 – display errors 1 – do not display errors	Yes	No
IgnoreRootDCErrors	REG_DWORD	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Change Summary footer: 0 – display errors 1 – do not display errors	Yes	No
MonitorModifiedAndRevertedBack	REG_DWORD	Defines whether the Change Summary must display the attributes whose values were modified and then restored between data collections: 0 – these attributes are not displayed 1 – these attributes are displayed as "modified and reverted back"	No	No

Registry Key	Type	Description/Values	Created on installation	Preserved during upgrade
ShortEmailSubjects	REG_DWORD	Defines whether to contract the email subjects (e.g. NetWrix Active Directory Change Reporter: Summary Report → ADCR Report): 0 – no 1 - yes	No	No
ProcessBackupLogs	REG_DWORD	Defines whether to process security log backups: 0 – no 1 – yes **Note**: Even if this key is set to 0, the security log backups will not be deleted regardless of the value of the CleanAutoBackupLogs key.	Yes	No
ShowReportFooter	REG_DWORD	Defines whether to display the footer in the Change Summary emails. 0 – no 1 - yes	Yes	No
ShowReportGeneratorServer	REG_DWORD	Defines whether to dsisplay the report generation server in the Change Summary footer: 0 – no 1 - yes	Yes	No
ShowSummaryInFooter	REG_DWORD	Defines whether to display summary information in the Change Summary footer: 0 – no 1 - yes	Yes	No
ShowSummaryInHeader	REG_DWORD	Defines whether to display summary information in the Change Summary header: 0 – no 1 - yes	Yes	No
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\NetWrix\AD Change Reporter\<Managed Object Name>				
CollectLogsMaxThreads	REG_DWORD	Defines the number of domain controllers to simultaneously start log collection on	No	Yes
HKEY_LOCAL_MACHINE\SOFTWARE\(WOW6432Node)\NetWrix\Management Console\Database settings				
overwrite_datasource	REG_DWORD	Defines whether to overwrite the database connection settings (stored in the reports data source) if they differ from the SQL server settings specified on Managed Object	No	Yes

Registry Key	Type	Description/Values	Created on installation	Preserved during upgrade
		configuration 0 – no 1 - yes		
SqlOperationTimeout	REG_DWORD	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds)	No	Yes
timeout	REG_DWORD	Defines the SQL database connection timeout (in seconds)	No	No

D APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support NetWrix Active Directory Change Reporter:

Table 15: Product Documentation

Document Name	Overview
NetWrix Active Directory Change Reporter Administrator's Guide	The current document.
NetWrix Active Directory Change Reporter Installation and Configuration Guide	Provides detailed instructions on how to install NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter, and explains how to configure the target AD domain for auditing.
NetWrix Active Directory 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 Active Directory Change Reporter User Guide	Provides the information on different NetWrix Active Directory Change Reporter reporting capabilities, lists all available reports and explains how they can be viewed and interpreted.
NetWrix Active Directory Change Reporter Freeware Edition Quick-Start Guide	Provides instructions on how to install, configure and use NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter Freeware Edition.
NetWrix Active Directory Change Reporter Release Notes	Contains a list of the known issues that customers may experience with NetWrix Active Directory Change Reporter 7.2, and suggests workarounds for these issues.
Troubleshooting Incorrect Reporting of the "Who Changed" Parameter	Step-by-step instructions on how to troubleshoot incorrect reporting of the 'who changed' parameter.
Configuring Real-Time Alerts in NetWrix Active Directory Change Reporter	This technical article provides detailed instructions on how to configure real-time alerts, as well as an algorithm for selecting the correct attribute for the type of change you want to track. It also contains step-by-step procedures that will guide you through configuration of some most commonly used alerts.
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.
Integration with Third Party SIEM Systems	This article explains how to enable integration with third-party Security Information and Event Management (SIEM) systems.
Native AD Auditing Cheat Sheet	Provides an Active Directory auditing configuration checklist.