NetWrix Group Policy Change Reporter

Administrator's Guide

Product Version: 7.2

November 2012

Copyright © 2012 NetWrix Corporation. All Rights Reserved.

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.

© 2012 NetWrix Corporation.

All rights reserved.

Table of Contents

Copyright © 2012 NetWrix Corporation. All Rights Reserved

Copyright © 2012 NetWrix Corporation. All Rights Reserved

1. Introduction

1.1. Overview

This guide contains an overview of the NetWrix Group Policy 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 Active Directory 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 Group Policy 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 Group Policy Change Reporter data collection workflow and contains detailed information on the Change Summary options and Sessions.
- Chapter 6 Reports: provides an overview of the Reports feature, explains how to configure and view reports and contains report examples. It also contains step-by-step instructions on how to configure subscriptions to Reports.
- Chapter 7 Configuring Global Settings: explains how to configure or modify the settings that are applied to all Managed Objects and all NetWrix modules enabled for these objects.
- Chapter 8 Additional Configuration: provides a description of the product additional configuration options, such as enabling integration with SIEM (Security Information and Event Management) solutions and excluding data types from data collection and product reports.
- A Appendix: Registry Keys: contains a table with description of the basic NetWrix Group Policy Change Reporter registry keys.
- B Appendix: Related Documentation: contains a list of all documentation published to support NetWrix Group Policy Change Reporter.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

2. Product Overview

Group Policy auditing is a must-have procedure for all organizations relying on Group Policy infrastructure. Relatively small changes to security policies, desktop configurations, software deployment and other settings can severely impact enterprise security, compliance, and performance. An uncontrolled and unaudited change process imposes major security and compliance risks for an IT infrastructure run by multiple IT professionals.

Built-in Group Policy management tools do not provide any auditing and change reporting capabilities, and it is just impossible to track the WHO, WHAT, WHERE and WHEN data for critical modifications by using these tools. For example, auditing with the native Windows tools can only indicate that a Group Policy changed, but it does not say WHAT setting has been changed; you can get only cryptic GUIDs for cross-referencing as a source of information.

Windows 2003 and earlier versions do not provide the before and after values for the Group Policy Object (GPO) link. Windows 2008 provides this data but it is difficult to use it efficiently. For detailed comparison of the native auditing tools and NetWrix products refer to Summary: Limitations of Native Active Directory Auditing Tools.

Powered by the NetWrix AuditAssurance™ technology, NetWrix Group Policy Change Reporter makes the Group Policy change auditing an easy and straightforward process, resulting in a complete and concise picture of all changes taking place in your monitored environment. AuditAssurance™ is a patent-pending technology that consolidates audit data from multiple independent sources such as event logs, configuration snapshots, change history records, and others. This allows detecting WHO changed WHAT, WHERE and WHEN, even if one or several sources of information do not contain all of the required data, for example because it was deleted, overwritten, and so on.

NetWrix Group Policy Change Reporter provides data on every single change made to the Group Policy configuration, including newly created and deleted GPOs, GPO link changes, changes made to audit policy, password policy, software deployment, user desktops, and other settings. The data includes detailed information for all changes with the previous and current values for all modified settings.

The product records all Group Policy modifications and archives them to enable historical reporting. You can build a summary of changes made to Group Policy during any period. For example, you can analyze any policy violations that took place in the past, see who turned off invalid logon auditing in your domain security policy, who added new software to deploy on client computers, who changed desktop firewall and lockdown settings, and so on.

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 Group Policy Change Reporter is a module included into a larger NetWrix Active Directory Change Reporter pack that automates auditing of the entire Active Directory infrastructure. The NetWrix Active Directory Change Reporter pack consists of the following modules:

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

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

2.1. Key Features and Benefits

NetWrix Group Policy Change Reporter is a tool for automated auditing and reporting on changes to Group Policy objects configuration in the monitored domain. It allows you to do the following:

- **Monitor day-to-day administrative activities**: the product captures detailed information on all changes made to Group Policy objects and their settings in the monitored Active Directory environment, including the information on WHO changed WHAT, WHEN and WHERE.
- **Sustain compliance** by using in-depth change information. Audit data can be archived and stored for more than 7 years to be used for reports generation.
- **Streamline change control**: paint the most complete picture of Group Policy security settings throughout Active Directory by monitoring all settings and permission changes.

The main NetWrix Group Policy Change Reporter features are:

- **Reports** with the previous and current values for every object- and setting-level change. Reports are based on SQL Server Reporting Services (SSRS) with over 40 predefined report templates and support for custom reports.
- **Report subscriptions** allow for scheduled report generation and delivery to the specified recipients. You can apply different report filters and select report output format.
- **Automatic Backup and Recovery of Group Policy Objects:** the product supports recovery of unwanted Group Policy objects 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.
- **Integration 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.

2.2. Product Workflow

A typical NetWrix Group Policy 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 Group Policy Change Reporter monitors AD domain and collects data on Group Policy changes. Audit data is written to a local file-based storage, referred to as the Audit Archive.

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

2.3. Product Editions

NetWrix Group Policy 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 (consisting of 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 difference between the NetWrix Group Policy Change Reporter editions:

Table 1: NetWrix Group Policy 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
Report Subscriptions	No	Yes
Integration with Microsoft System Center Operations Manager Pack (SCOM) (via NetWrix SCOM Management Pack for Group Policy Change Reporter)	No	Yes
Long-term archiving of audit data	No Data is only stored 4 days	Yes Any period of time
Daily Change Summary email reflecting the changes made during the last day	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

Copyright © 2012 NetWrix Corporation. All Rights Reserved

3. NetWrix Enterprise Management Console Overview

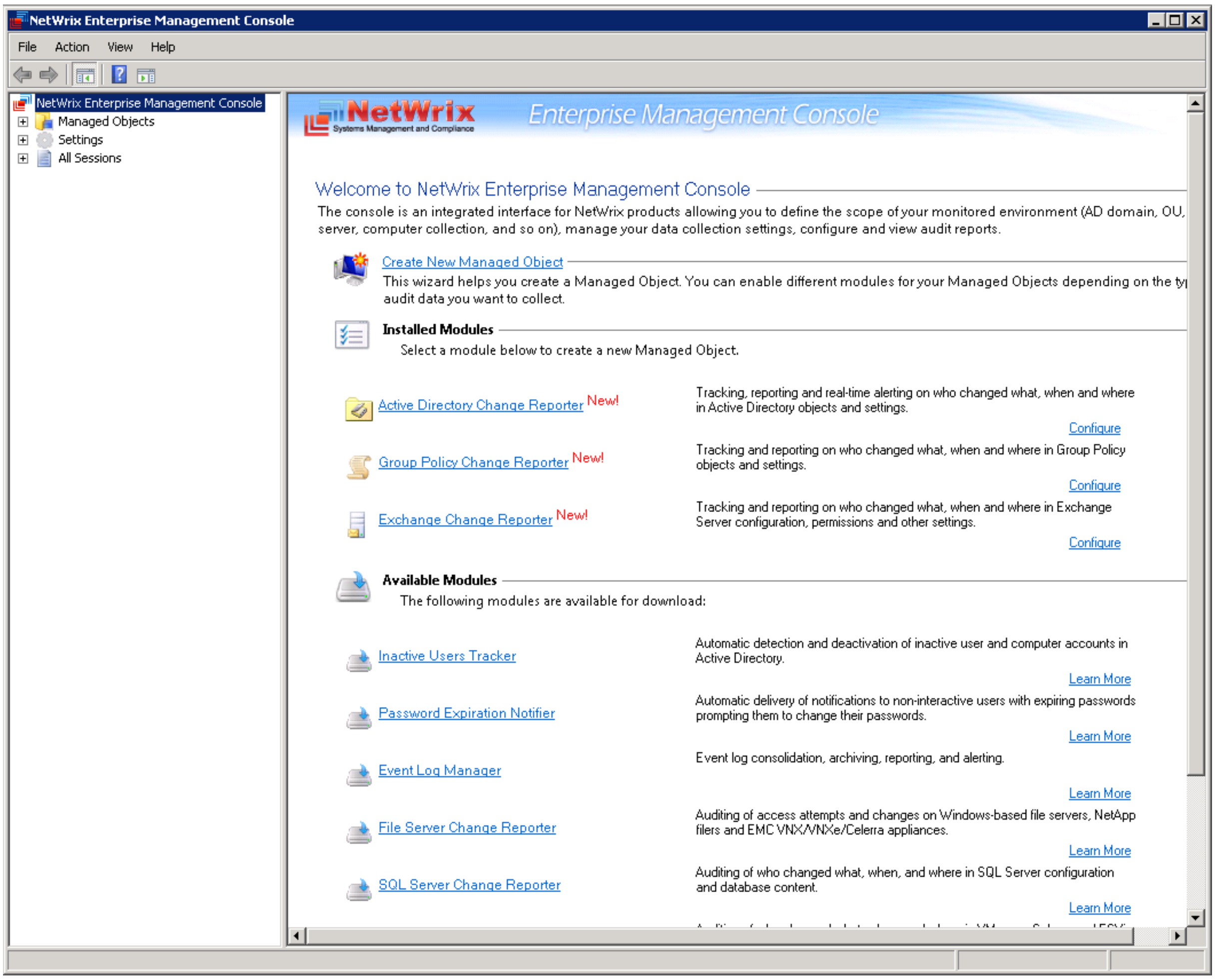
NetWrix Group Policy Change Reporter Enterprise Edition is integrated into NetWrix Enterprise Management Console, an MMC snap-in that allows configuring Managed Objects and their settings, and the reporting options.

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 → Group Policy Change Reporter** and click **Group Policy Change Reporter (Enterprise Edition)**. The Enterprise Management Console main page will be displayed:

Figure 1: NetWrix Enterprise Management Console


NetWrix Enterprise Management Console
File
Action
View
Help
NetWrix Enterprise Management Console
Managed Objects
Settings
All Sessions
NetWrix
Systems Management and Compliance
Enterprise Management Console

Welcome to NetWrix Enterprise Management Console

The console is an integrated interface for NetWrix products allowing you to define the scope of your monitored environment (AD domain, OU, server, computer collection, and so on), manage your data collection settings, configure and view audit reports.

Create New Managed Object

This wizard helps you create a Managed Object. You can enable different modules for your Managed Objects depending on the ty audit data you want to collect.

Installed Modules

Select a module below to create a new Managed Object.

Active Directory Change Reporter New!
Tracking, reporting and real-time alerting on who changed what, when and where in Active Directory objects and settings.
Configure

Group Policy Change Reporter New!
Tracking and reporting on who changed what, when and where in Group Policy objects and settings.
Configure

Exchange Change Reporter New!
Tracking and reporting on who changed what, when and where in Exchange Server configuration, permissions and other settings.
Configure

Available Modules

The following modules are available for download:

Inactive Users Tracker
Automatic detection and deactivation of inactive user and computer accounts in Active Directory.
Learn More

Password Expiration Notifier
Automatic delivery of notifications to non-interactive users with expiring passwords prompting them to change their passwords.
Learn More

Event Log Manager
Event log consolidation, archiving, reporting, and alerting.
Learn More

File Server Change Reporter
Auditing of access attempts and changes on Windows-based file servers, NetApp filers and EMC VNX/VNXe/Celerra appliances.
Learn More

SQL Server Change Reporter
Auditing of who changed what, when, and where in SQL Server configuration and database content.
Learn More

Copyright © 2012 NetWrix Corporation. All Rights Reserved

4. MANAGED OBJECT

In NetWrix Group Policy 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:

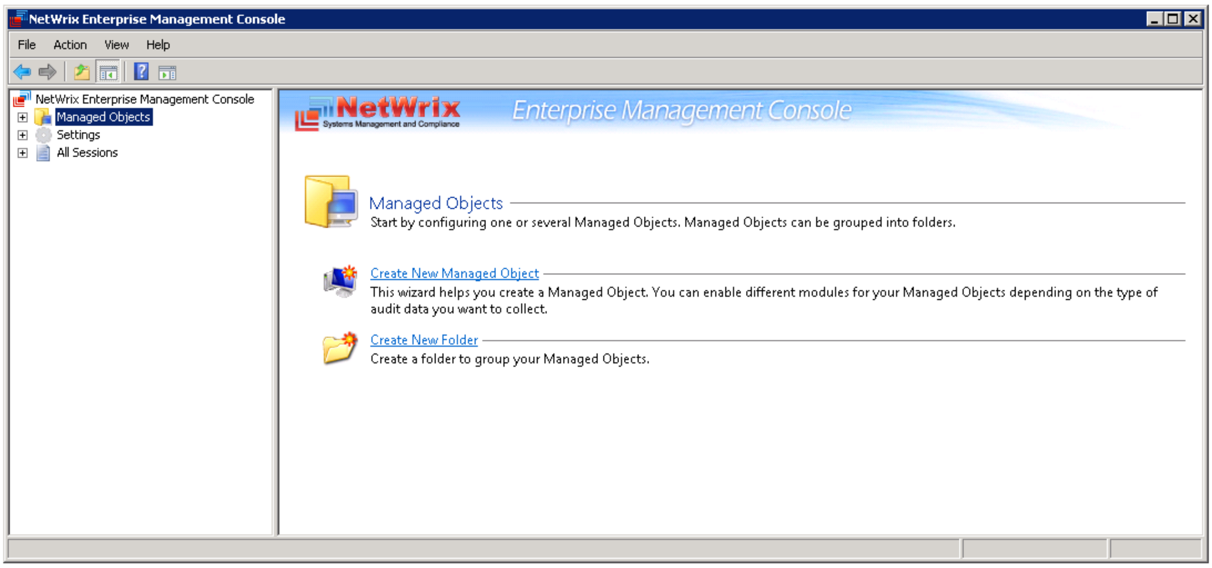
- Create and configure a Managed Object
- Modify Managed Object settings

4.1. Creating Managed Object

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: The Managed Objects Page


NetWrix Enterprise Management Console
File
Action
View
Help
NetWrix Enterprise Management Console
Managed Objects
Settings
All Sessions
NetWrix
Systems Management and Compliance
Enterprise Management Console

Managed Objects

Start by configuring one or several Managed Objects. Managed Objects can be grouped into folders.

Create New Managed Object

This wizard helps you create a Managed Object. You can enable different modules for your Managed Objects depending on the type of audit data you want to collect.

Create New Folder

Create a folder to group your Managed Objects.

2. In the right pane, click **Create New Managed Object**. Alternatively, right-click the **Managed Objects** node and select **New Managed Object** from the pop-up menu to start the **New Managed Object** wizard.

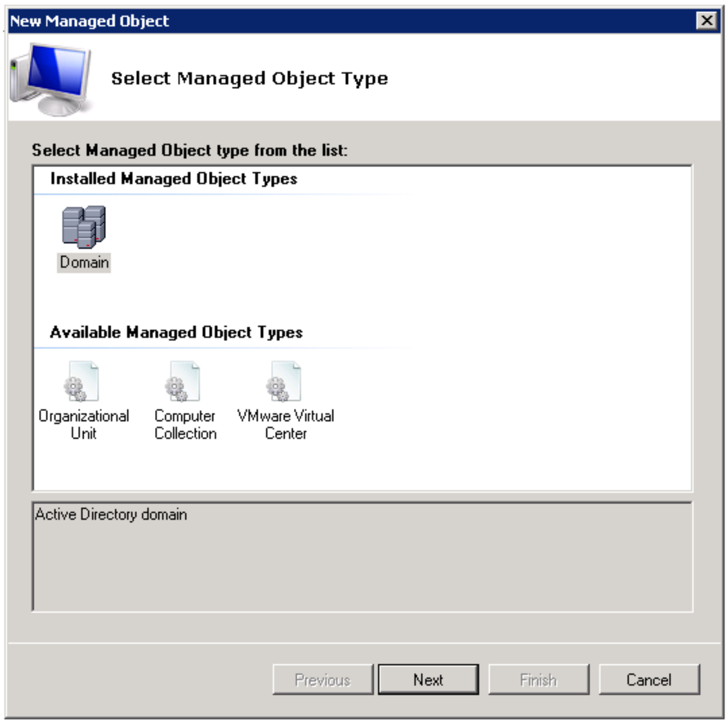
   Note: For your convenience, you can group Managed Objects into folders. To create a folder, right-click the **Managed Objects** node, select **New Folder**, and specify the folder name. Then create a new Managed Object inside this folder. You cannot move existing Managed Objects into folders once they 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.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

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 account and email settings on their configuration, the **Default Account** and **Configure Email Settings** steps of the wizard will be omitted.

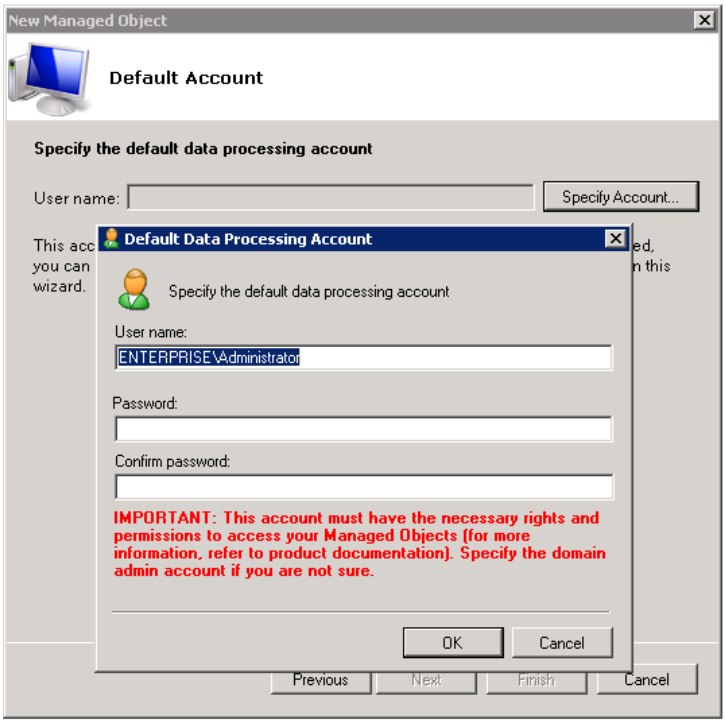
5. In the dialog that opens, enter the default Data Processing Account credentials that will be used by NetWrix Group Policy Change Reporter for data collection. The name should be specified in the following format: domain_name\account_name. This account must have the following rights:

   - Local administrator on the computer where NetWrix Group Policy 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 will 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.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

Figure 4: New Managed Object: Default Account



New Managed Object

Default Account

Specify the default data processing account

User name:

This acc... you can ... wizard. ...ed, ...n this

Default Data Processing Account

Specify the default data processing account

User name: ENTERPRISE\Administrator

Password:

Confirm password:

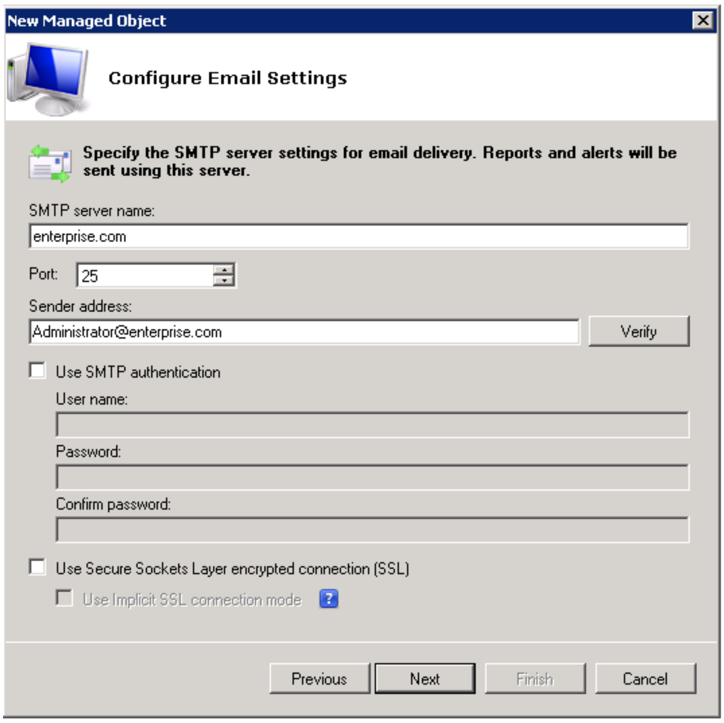
IMPORTANT: This account must have the necessary rights and permissions to access your Managed Objects (for more information, refer to product documentation). Specify the domain admin account if you are not sure.

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 21 To modify Data Processing Account settings).

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

Figure 5: New Managed Object: Configure Email Settings



New Managed Object

Configure Email Settings

Specify the SMTP server settings for email delivery. Reports and alerts will be sent using this server.

SMTP server name: enterprise.com

Port: 25

Sender address: Administrator@enterprise.com

☐ Use SMTP authentication

User name:

Password:

Confirm password:

☐ Use Secure Sockets Layer encrypted connection (SSL)

☐ Use Implicit SSL connection mode

The following parameters must be specified:

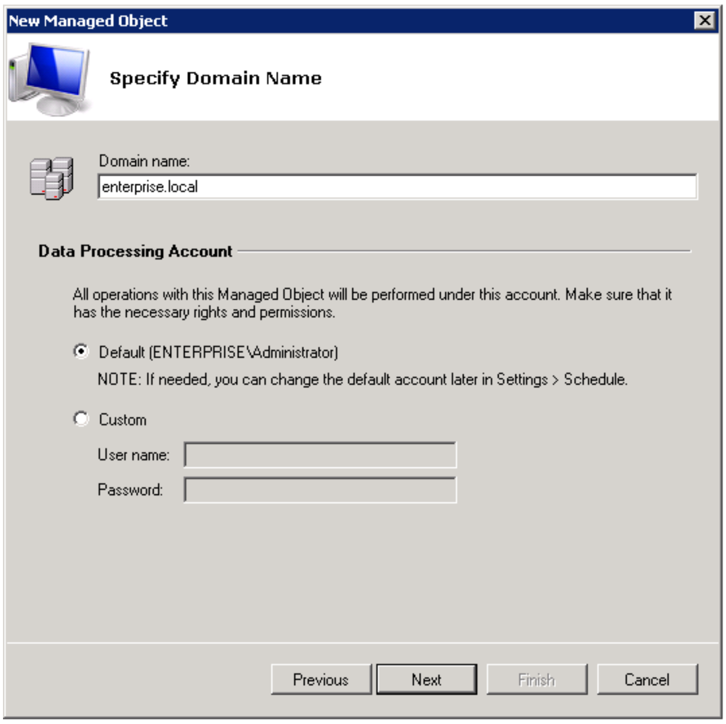
Table 2: Email Settings Parameters

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 check box if your SMTP server requires SSL to be enabled.
Use Implicit SSL connection mode	Select this check box 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, in NetWrix Enterprise Management Console, navigate to **Settings → Email Notifications**. In the right pane, click the **Configure** button and edit the required parameters. For instructions, refer to Procedure 19 To configure the email notifications settings.

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

Figure 6: New Managed Object: Specify Domain Name



Domain name: enterprise.local

Data Processing Account

All operations with this Managed Object will be performed under this account. Make sure that it has the necessary rights and permissions.

● Default (ENTERPRISE\Administrator)

NOTE: If needed, you can change the default account later in Settings > Schedule.

○ Custom

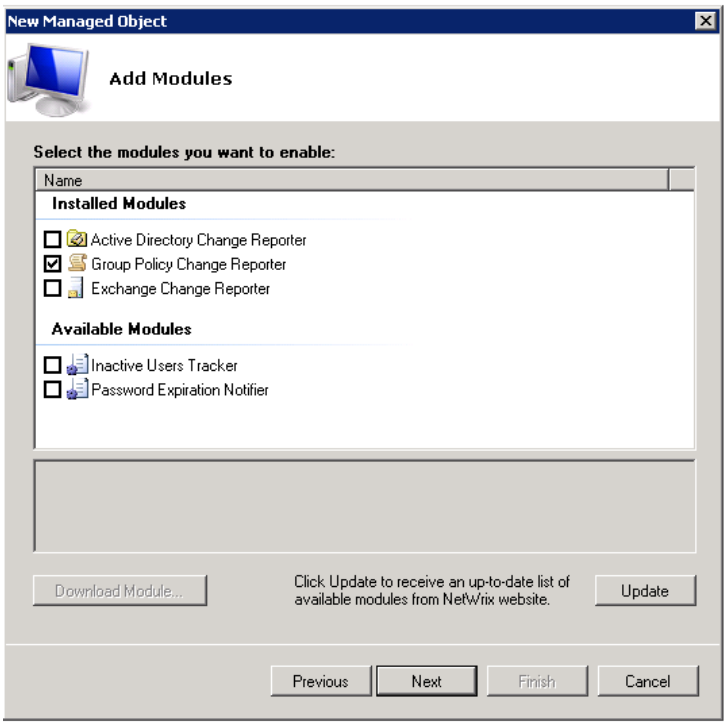
User name:

Password:

If you want to use a specific account to access data from this domain (other than the one you have 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.

8. On the **Add Modules** step, make sure the Group Policy Change Reporter module is selected under **Installed Modules**:

Figure 7: New Managed Object: Add Modules


New Managed Object

Add Modules

Select the modules you want to enable:

Name

Installed Modules

☐ Active Directory Change Reporter
☑ Group Policy Change Reporter
☐ Exchange Change Reporter

Available Modules

☐ Inactive Users Tracker
☐ Password Expiration Notifier

Click Update to receive an up-to-date list of available modules from NetWrix website.

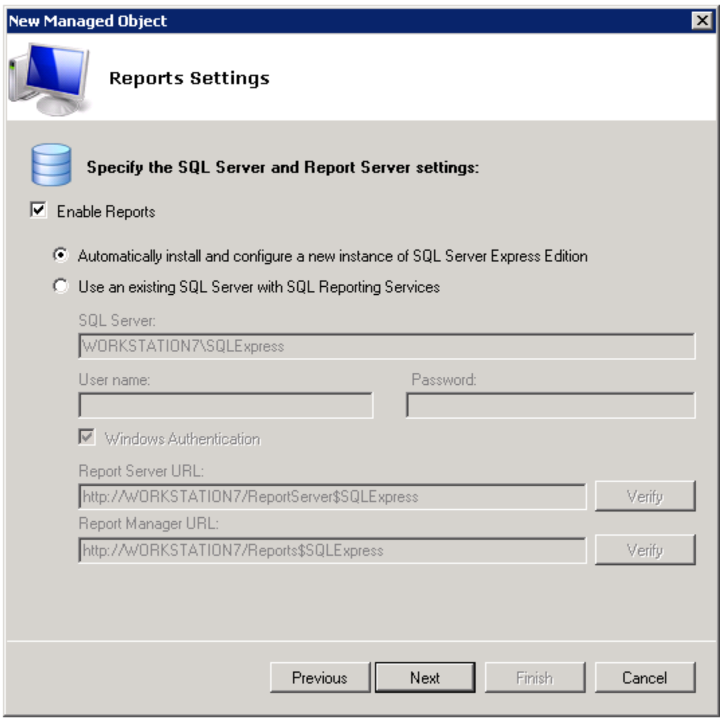
Note: If you have installed other NetWrix change reporting products previously, the list of **Installed Modules** may contain several options.

On this step, under **Available Modules**, there is a list of other NetWrix products that can have domain as a Managed Object type. To get more information on these products and download them, select the corresponding check box, or click a module and then click the **Download Module** button. You will be redirected to the product website page.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

9. On the **Reports Settings** step, select the **Enable Reports** check box if you want to use the SSRS-based Reports:

Figure 8: New Managed Object: Reports Settings



New Managed Object

Reports Settings

Specify the SQL Server and Report Server settings:

☑ Enable Reports

● Automatically install and configure a new instance of SQL Server Express Edition

○ Use an existing SQL Server with SQL Reporting Services

SQL Server: WORKSTATION7\SQLExpress

User name:

Password:

☑ Windows Authentication

Report Server URL: http://WORKSTATION7/ReportServer$SQLExpress

Report Manager URL: http://WORKSTATION7/Reports$SQLExpress

Note: If you do not enable the **Reports** feature, audit data will not be written to an SQL database. You can enable and configure the feature later (for details, refer to Section 6.2 Configuring Reports).

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 Group Policy 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.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

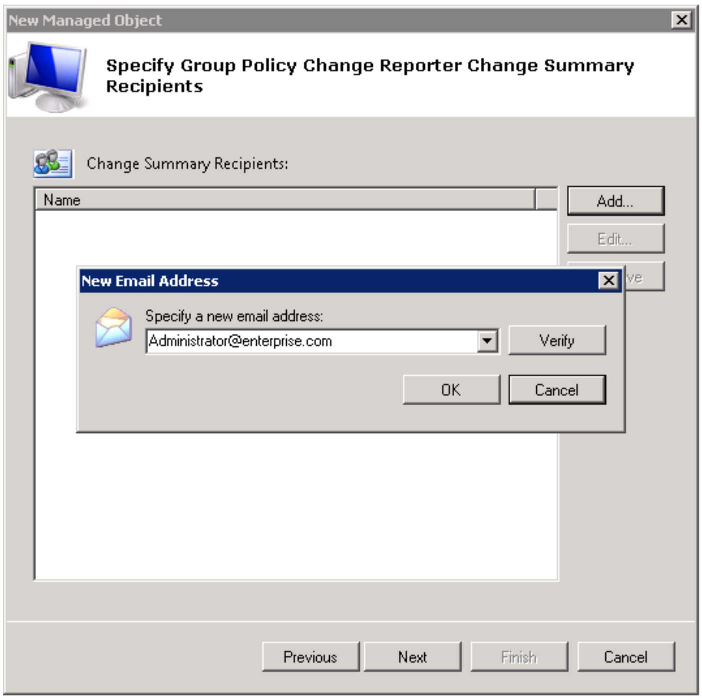
User name	Specify a user name for the SQL Server authentication. **NOTE:** This user must belong to the target database owner (dbo) role. For instructions on how to assign this role to a user, refer to Section 6.2.1. Configuring Rights and Permissions of NetWrix Active Directory Change Reporter Installation 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 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.

Note: If you have already created other Managed Objects, and configured the Reports settings for them, on this step you will only be prompted to enable or disable the Reports feature. If you want to use custom Reports settings for this Managed Object (for example, write data to a different SQL database), you can change the Reports settings later (for instructions, refer to 6.2.1 Configuring SQL Server Settings).

Click **Next** to continue and wait until NetWrix Enterprise Management Console has established a connection with the Report Server.

10. On the **Specify Group Policy Change Reporter Change Summary Recipients** step, click the **Add** button to specify the Change Summary recipient(s):

Figure 9: New Managed Object: Specify Change Summary Recipients



New Managed Object
Specify Group Policy Change Reporter Change Summary Recipients
Change Summary Recipients:
Name
Add...
Edit...
ve
New Email Address
Previous
Next
Finish
Cancel

Specify a new email address: Administrator@enterprise.com

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**. If your audit settings have not been configured properly, you will receive a warning message. For detailed instructions on

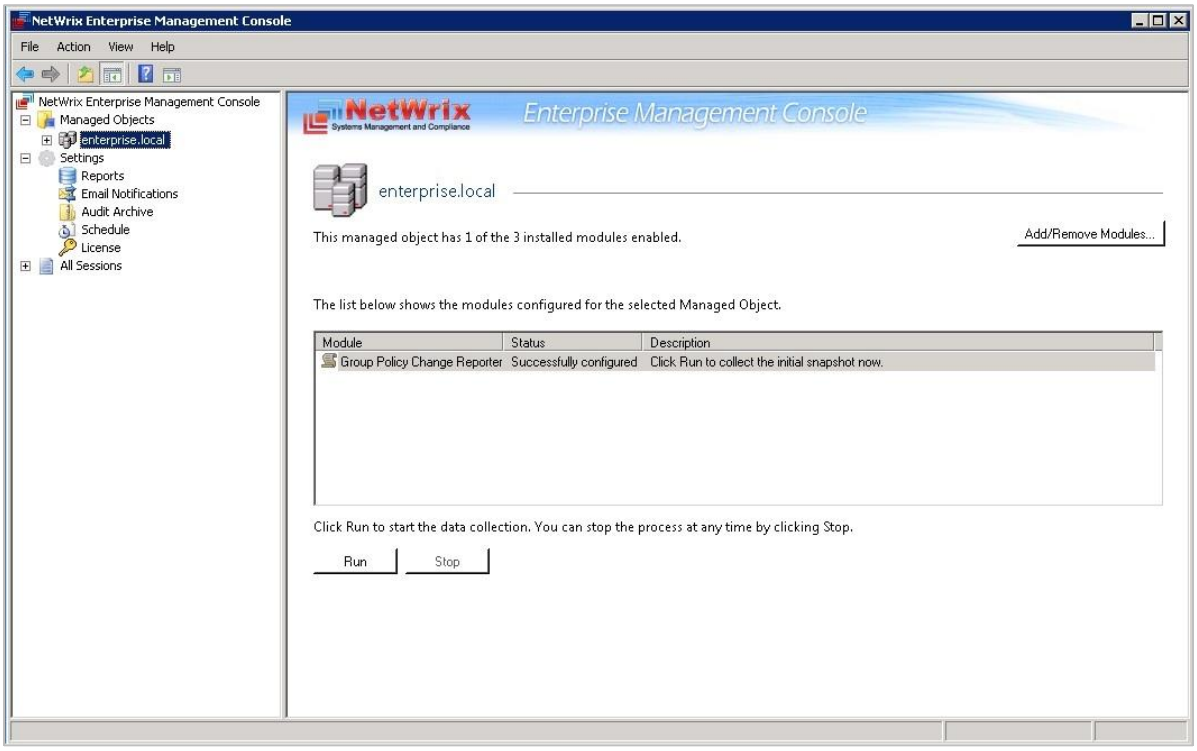
Copyright © 2012 NetWrix Corporation. All Rights Reserved

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.

11. On the last step, review your Managed Object settings and click **Finish.** 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 10: The Managed Object Page



enterprise.local

This managed object has 1 of the 3 installed modules enabled.

The list below shows the modules configured for the selected Managed Object.

Module	Status	Description
Group Policy Change Reporter	Successfully configured	Click Run to collect the initial snapshot now.

Click Run to start the data collection. You can stop the process at any time by clicking Stop.

4.2. Modifying Managed Object Settings

To modify the settings for an existing Managed Object, perform one of the following procedures:

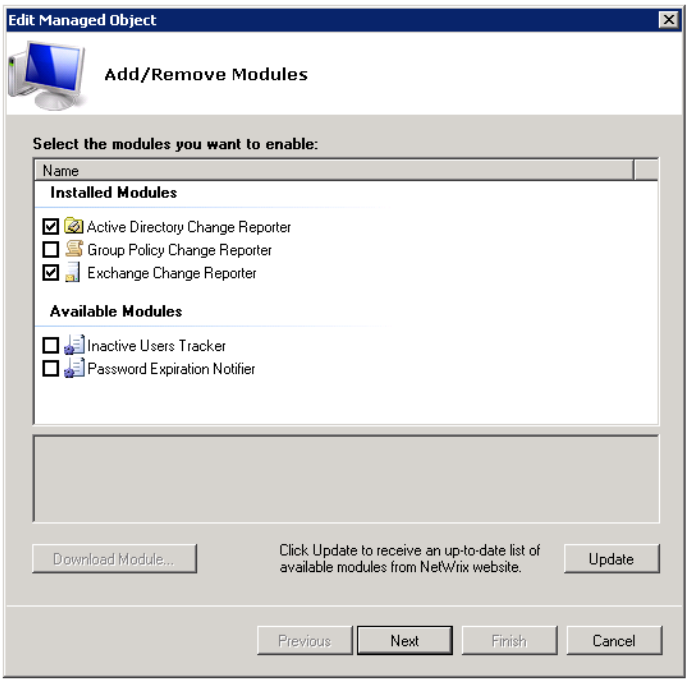
- To modify general settings: add or remove NetWrix modules for the selected Managed Object.
- To modify the Data Processing Account: override the default Data Processing Account for this Managed Object and specify a different account for data collection.
- To modify Group Policy Change Reporter settings.

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 Details page will be displayed showing a list of NetWrix modules added for this Managed Object.
2. Click the Add/Remove button. The Edit Managed Object wizard will start with the **Add/Remove Modules** screen.
3. In the **Installed Modules** list, select or clear the required module check box to add the module or remove it respectively. Click **Next**:

Copyright © 2012 NetWrix Corporation. All Rights Reserved

Figure 11: Add/Remove Modules



Edit Managed Object

Add/Remove Modules

Select the modules you want to enable:

Installed Modules

- ☑ Active Directory Change Reporter
- □ Group Policy Change Reporter
- ☑ Exchange Change Reporter

Available Modules

- □ Inactive Users Tracker
- □ Password Expiration Notifier

Click Update to receive an up-to-date list of available modules from NetWrix website.

4. The **Available Modules** list contains all NetWrix products that can have domain as a Managed Object type. To get more information on these products and download them, select the corresponding check box, or click a module and then click the **Download Module** button. You will be redirected to the product website page.

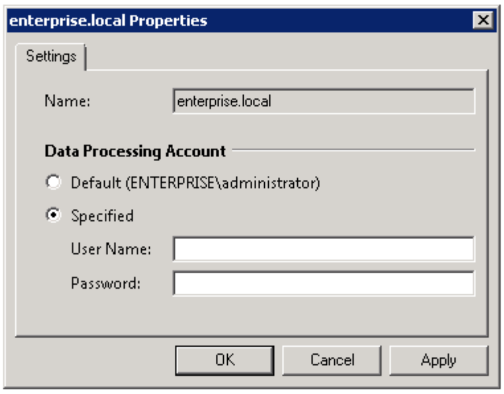
5. Follow the steps of the wizard to configure the selected module for your Managed Object. For detailed instructions, refer to the procedure explaining how to create and configure a Managed Object in the relevant NetWrix product Administrator's guide.

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 pop-up menu.

2. In the dialog that opens, select the **Specified** option under **Data Processing Account** and specify the credentials:

Figure 12: Managed Object Properties



enterprise.local Properties

Name: enterprise.local

Data Processing Account

○ Default (ENTERPRISE\administrator)

● Specified

User Name:

Password:

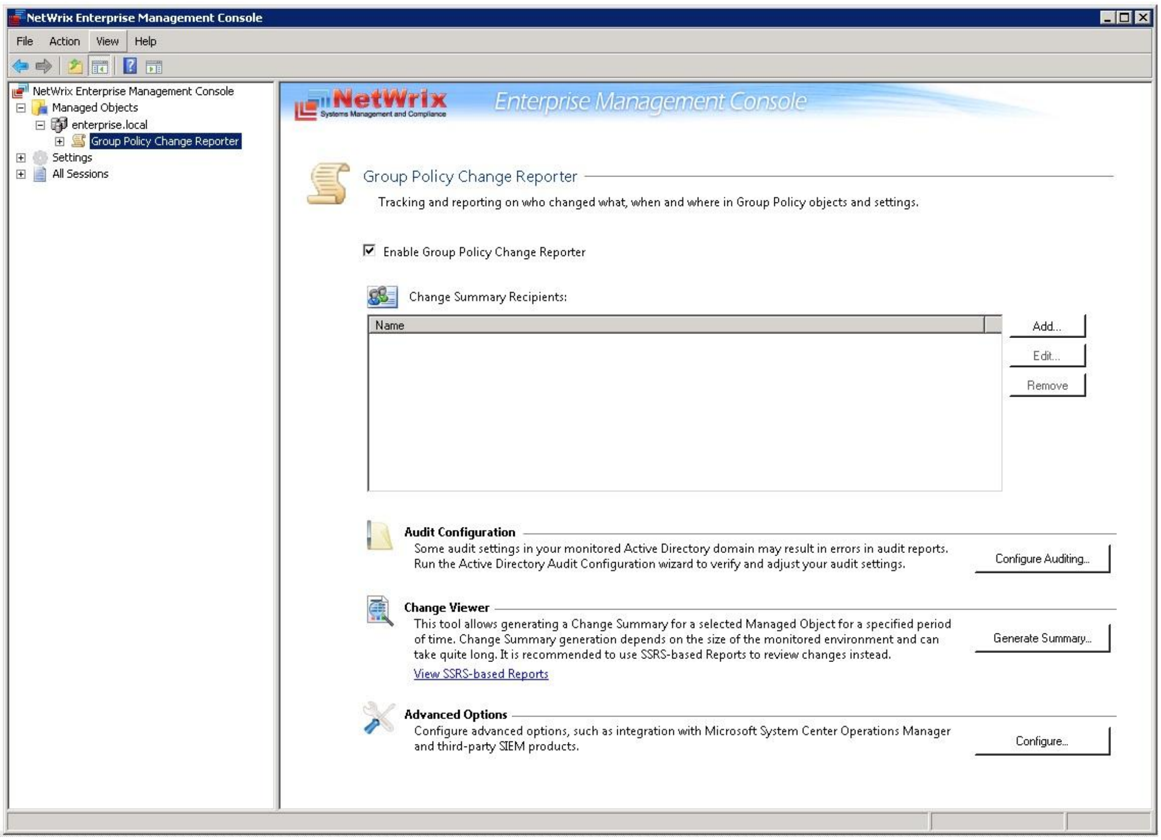
3. Click **OK** to save the changes. This account will be used for data collection from this Managed Object.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

Procedure 4. To modify Group Policy Change Reporter settings

1. In NetWrix Enterprise Management Console, navigate to **Managed Objects** → **<Managed_Object_name>** and select **Group Policy Change Reporter**. The NetWrix Group Policy Change Reporter settings page will be displayed:

Figure 13: Group Policy Change Reporter Settings Page



NetWrix Enterprise Management Console
File
Action
View
Help
NetWrix Enterprise Management Console
Managed Objects
enterprise.local
Group Policy Change Reporter
Settings
All Sessions
NetWrix Systems Management and Compliance
Enterprise Management Console
Name
Add...
Edit...
Remove
Configure Auditing...
Generate Summary...
Configure...

Group Policy Change Reporter

Tracking and reporting on who changed what, when and where in Group Policy objects and settings.

☑ Enable Group Policy Change Reporter

Change Summary Recipients:

Audit Configuration

Some audit settings in your monitored Active Directory domain may result in errors in audit reports. Run the Active Directory Audit Configuration wizard to verify and adjust your audit settings.

Change Viewer

This tool allows generating a Change Summary for a selected Managed Object for a specified period of time. Change Summary generation depends on the size of the monitored environment and can take quite long. It is recommended to use SSRS-based Reports to review changes instead.

View SSRS-based Reports

Advanced Options

Configure advanced options, such as integration with Microsoft System Center Operations Manager and third-party SIEM products.

2. Modify the NetWrix Group Policy Change Reporter settings as follows:

- To enable or disable the module, select or clear respectively the **Enable Group Policy Change Reporter** check box.
- To add a new recipient to the **Change Summary Recipients** list, click the **Add** button. In the dialog that opens, specify an email address and click **OK**. It is recommended to click the **Verify** button to check the email address. The system will send a test message to the specified address 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 adjust your audit settings, click the **Configure Auditing** button.
- To generate Change Summary on a particular Managed Object for a specific period of time, click the **Generate Summary** button. For details, refer to Procedure 6 To generate Change Summary on Demand.
- To use the advanced product options, click the **Configure** button. For details, refer to Procedure 23 To enable integration with third-party SIEM solutions.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

5. DATA COLLECTION

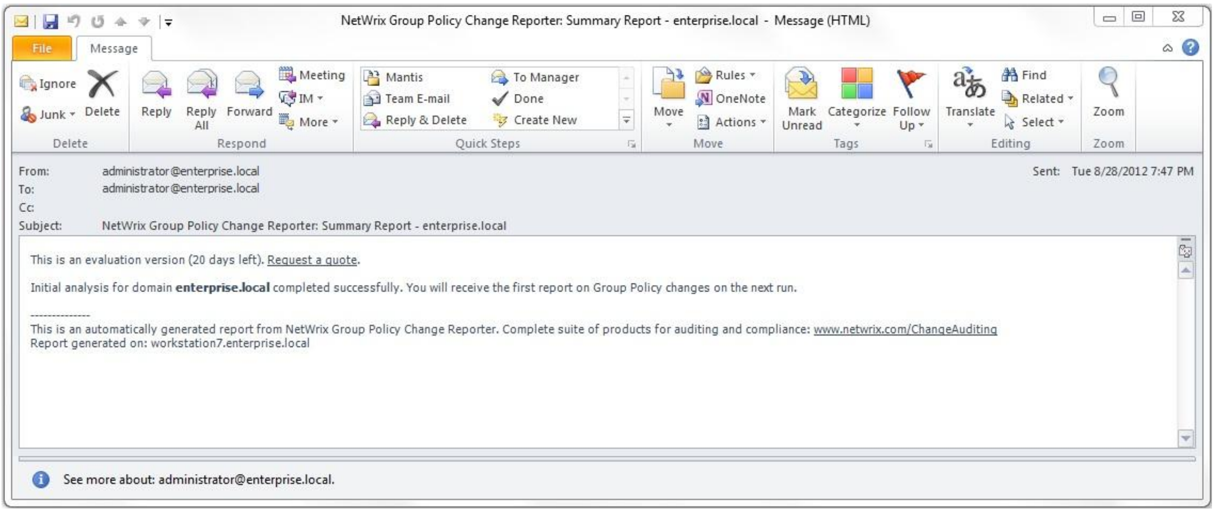
5.1. Data Collection Workflow

NetWrix Group Policy Change Reporter data collection workflow is as follows:

1. When a new Managed Object is created, NetWrix Group Policy Change Reporter starts collecting data from the monitored domain. The first data collection creates an initial snapshot of your monitored domain current state. NetWrix Group Policy 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):

Figure 14: Initial Analysis Notification



From: administrator@enterprise.local

To: administrator@enterprise.local

Cc:

Subject: NetWrix Group Policy Change Reporter: Summary Report - enterprise.local

Sent: Tue 8/28/2012 7:47 PM

This is an evaluation version (20 days left). Request a quote.

Initial analysis for domain **enterprise.local** completed successfully. You will receive the first report on Group Policy changes on the next run.

This is an automatically generated report from NetWrix Group Policy Change Reporter. Complete suite of products for auditing and compliance: www.netwrix.com/ChangeAuditing
Report generated on: workstation7.enterprise.local

See more about: administrator@enterprise.local.

3. Once a day (at 3:00 AM by default), NetWrix Group Policy Change Reporter writes data on the detected changes to a local storage of audit data, the Audit Archive. If the Reports feature is enabled and configured, data is imported from the Audit Archive to an SQL database.

4. At the same time, the product generates and emails a Change Summary to the specified recipients.

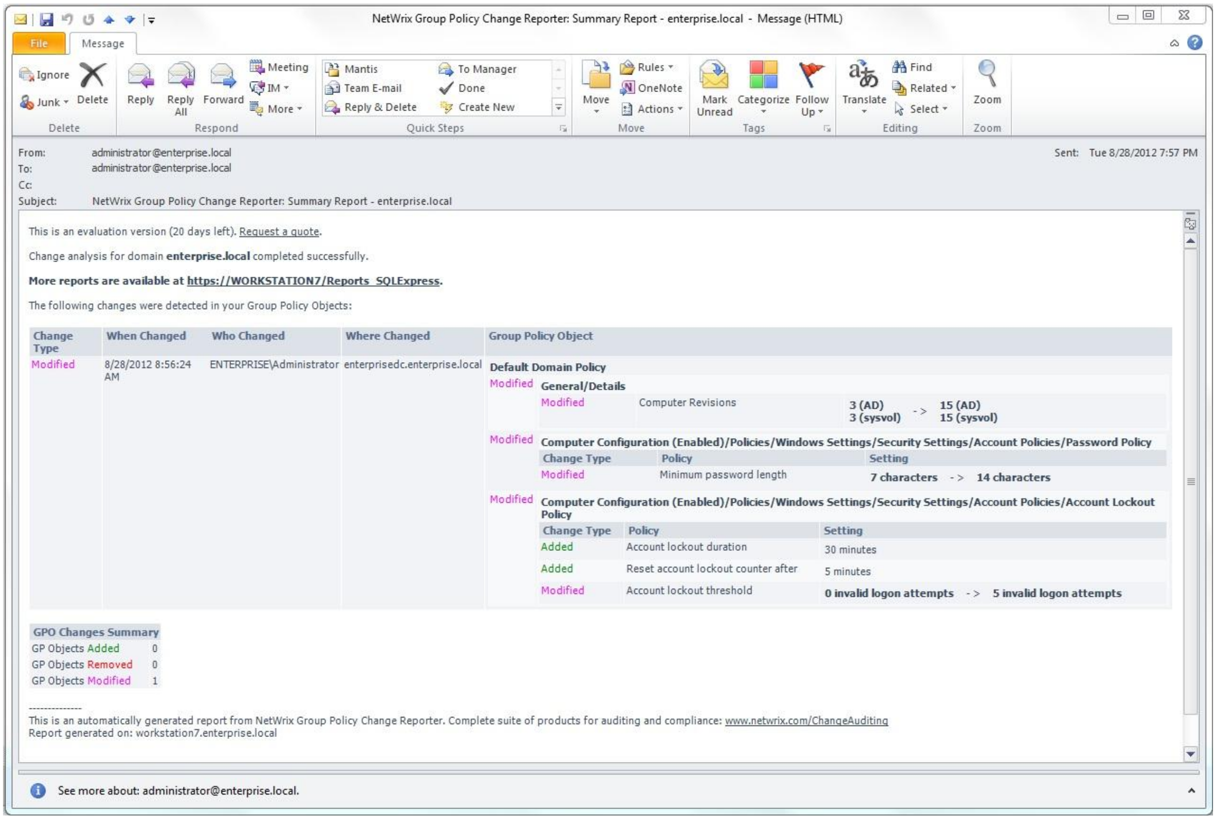
Note: For NetWrix Group Policy Change Reporter to be able to collect audit data successfully, you need to configure your monitored Active Directory domain for audit prior to using the product. For detailed instructions on how to do this, refer to Chapter 6. Configuring Target Environment of NetWrix Active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

Copyright © 2012 NetWrix Corporation. All Rights Reserved

5.2. Change Summary

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

Figure 15: Change Summary Example



From: administrator@enterprise.local

To: administrator@enterprise.local

Cc:

Subject: NetWrix Group Policy Change Reporter: Summary Report - enterprise.local

Sent: Tue 8/28/2012 7:57 PM

This is an evaluation version (20 days left). Request a quote.

Change analysis for domain **enterprise.local** completed successfully.

More reports are available at https://WORKSTATION7/Reports_SQLExpress.

The following changes were detected in your Group Policy Objects:

Change Type	When Changed	Who Changed	Where Changed	Group Policy Object
Modified	8/28/2012 8:56:24 AM	ENTERPRISE\Administrator	enterprisedc.enterprise.local	**Default Domain Policy**

Modified **General/Details**

Modified	Computer Revisions	**3 (AD)** **3 (sysvol)**	->	**15 (AD)** **15 (sysvol)**

Modified **Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Password Policy**

Change Type	Policy	Setting
Modified	Minimum password length	**7 characters** -> **14 characters**

Modified **Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Account Lockout Policy**

Change Type	Policy	Setting
Added	Account lockout duration	30 minutes
Added	Reset account lockout counter after	5 minutes
Modified	Account lockout threshold	**0 invalid logon attempts** -> **5 invalid logon attempts**

GPO Changes Summary	
GP Objects Added	0
GP Objects Removed	0
GP Objects Modified	1

This is an automatically generated report from NetWrix Group Policy Change Reporter. Complete suite of products for auditing and compliance: www.netwrix.com/ChangeAuditing
Report generated on: workstation7.enterprise.local

See more about: administrator@enterprise.local.

It provides the following information:

Table 4: Change Summary Fields

Parameter	Description
Change Type	Shows the type of action that was performed on the GP object. The values are: • Added • Removed • Modified
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 from which the change was made.
Group Policy Object	Shows the Group Policy Object that was changed with details on its "before" and "after" values.

5.2.1. Modifying Change Summary Delivery Schedule

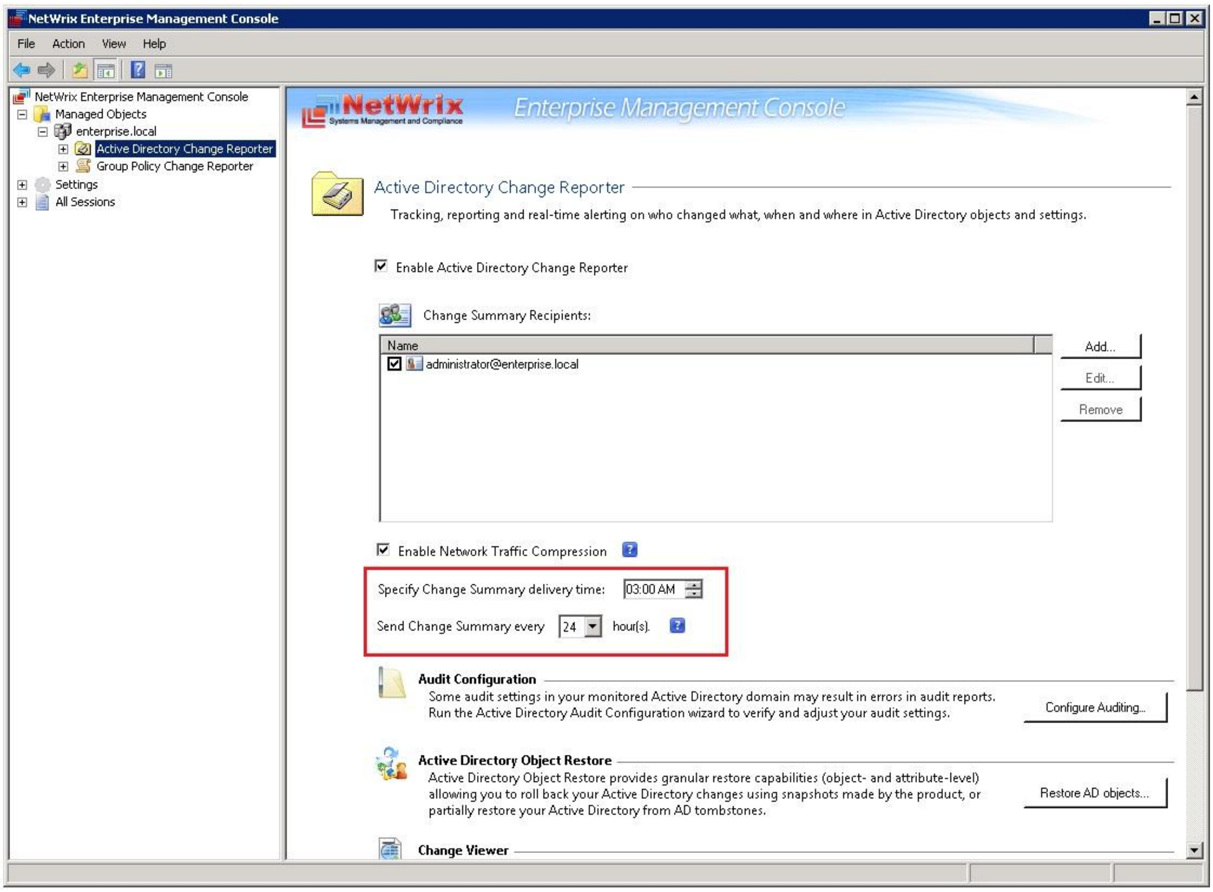
The Change Summary delivery schedule can only be modified if the Active Directory Change Reporter module is enabled for your Managed Object.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

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:**

Figure 16: The Active Directory Change Reporter Page



NetWrix Enterprise Management Console
File Action View Help
NetWrix Enterprise Management Console
Managed Objects
enterprise.local
Active Directory Change Reporter
Group Policy Change Reporter
Settings
All Sessions
NetWrix Systems Management and Compliance
Enterprise Management Console

Active Directory Change Reporter

Tracking, reporting and real-time alerting on who changed what, when and where in Active Directory objects and settings.

☑ Enable Active Directory Change Reporter

Change Summary Recipients:

Name
☑ administrator@enterprise.local

☑ Enable Network Traffic Compression

Specify Change Summary delivery time: 03:00 AM

Send Change Summary every 24 hour(s).

Audit Configuration

Some audit settings in your monitored Active Directory domain may result in errors in audit reports. Run the Active Directory Audit Configuration wizard to verify and adjust your audit settings.

Active Directory Object Restore

Active Directory Object Restore provides granular restore capabilities (object- and attribute-level) allowing you to roll back your Active Directory changes using snapshots made by the product, or partially restore your Active Directory from AD tombstones.

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.

Note: The changes will be applied to all modules of the NetWrix Active Directory Change Reporter pack enabled for the selected Managed Object.

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 10: The 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).

Copyright © 2012 NetWrix Corporation. All Rights Reserved

Note: Depending on the size of the monitored environement and the number of changes, Change Summary generation may take quite long.

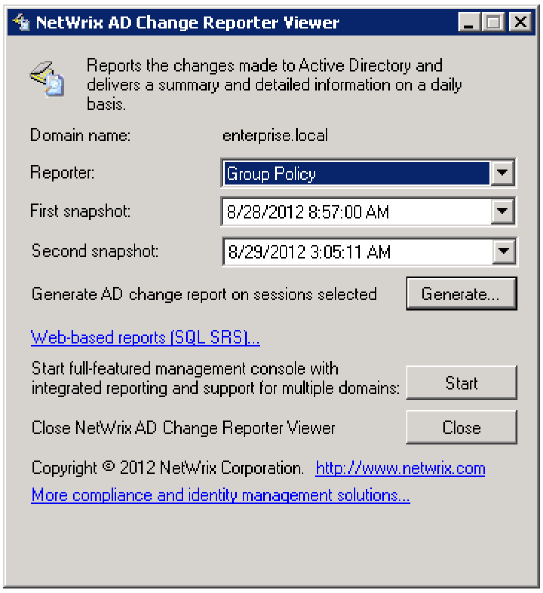
5.2.3. Viewing Change Summary for a Specified Date Range

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> → Group Policy Change Reporter.
2. In the right pane, click the **Generate Summary** button next to **Change Viewer**. The Change Viewer tool will open:

Figure 17: NetWrix AD Change Reporter Viewer



NetWrix AD Change Reporter Viewer

Reports the changes made to Active Directory and delivers a summary and detailed information on a daily basis.

Domain name: enterprise.local

Reporter: Group Policy

First snapshot: 8/28/2012 8:57:00 AM

Second snapshot: 8/29/2012 3:05:11 AM

Generate AD change report on sessions selected

Web-based reports (SQL SRS)...

Start full-featured management console with integrated reporting and support for multiple domains:

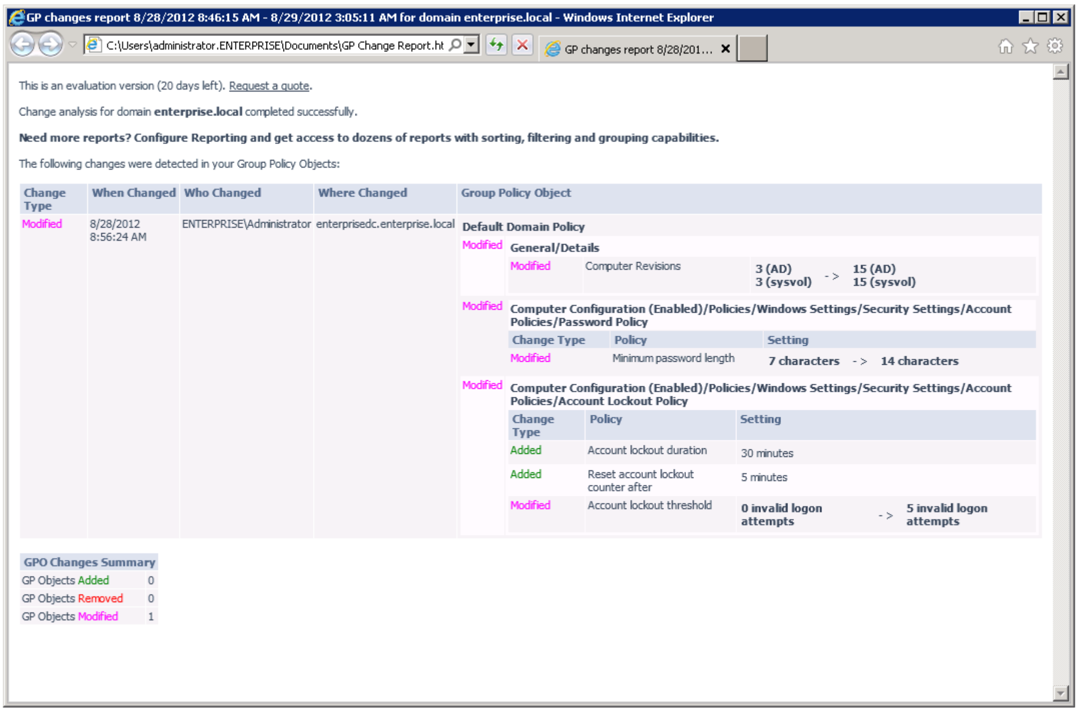
Close NetWrix AD Change Reporter Viewer

Copyright © 2012 NetWrix Corporation. http://www.netwrix.com

More compliance and identity management solutions...

3. Make sure **Group Policy** is selected in the **Reporter** drop-down list.
4. Specify the date range by selecting NetWrix Group Policy Change Reporter snapshots in the **First snapshot** and **Second snapshot** drop-down lists.
5. Click the **Generate** button.
6. In the **Save as** dialog, specify the location where the Change Summary will be saved. By default, the html file is saved in the user's **Documents** folder.
7. Once generated, the Change Summary will be displayed in your default web browser:

Figure 18: Change Summary for a Specific Date Range



GP changes report 8/28/2012 8:46:15 AM - 8/29/2012 3:05:11 AM for domain enterprise.local - Windows Internet Explorer

C:\Users\administrator.ENTERPRISE\Documents\GP Change Report.ht

GP changes report 8/28/201...

This is an evaluation version (20 days left). Request a quote.

Change analysis for domain **enterprise.local** completed successfully.

Need more reports? Configure Reporting and get access to dozens of reports with sorting, filtering and grouping capabilities.

The following changes were detected in your Group Policy Objects:

Change Type	When Changed	Who Changed	Where Changed	Group Policy Object
Modified	8/28/2012 8:56:24 AM	ENTERPRISE\Administrator	enterprisedc.enterprise.local	**Default Domain Policy**

Modified **General/Details**

Modified	Computer Revisions	**3 (AD)** **3 (sysvol)**	->	**15 (AD)** **15 (sysvol)**

Modified **Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Password Policy**

Change Type	Policy	Setting		
Modified	Minimum password length	**7 characters**	->	**14 characters**

Modified **Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Account Lockout Policy**

Change Type	Policy	Setting		
Added	Account lockout duration	30 minutes		
Added	Reset account lockout counter after	5 minutes		
Modified	Account lockout threshold	**0 invalid logon attempts**	->	**5 invalid logon attempts**

GPO Changes Summary	
GP Objects Added	0
GP Objects Removed	0
GP Objects Modified	1

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.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

5.3. Sessions

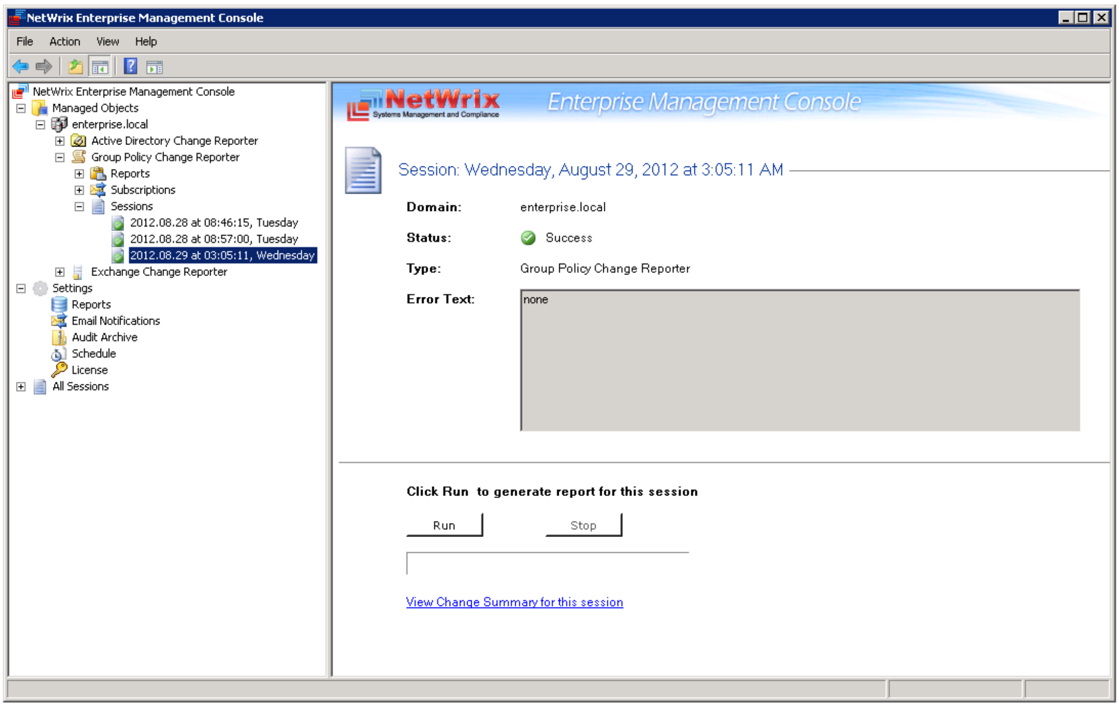
A Session is a scheduled or on-demand data collection that triggers Change Summary generation and delivery.

You can view Sessions in two ways:

- Under a particular Managed Object and NetWrix module enabled for it: in NetWrix Enterprise Management Console navigate to **Managed Objects** → **<Managed_Object_name>** → **Group Policy 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 a particular Session is selected in the tree, its details are displayed in the right pane:

Figure 19: The Session Details Page



NetWrix Enterprise Management Console
File
Action
View
Help
NetWrix Enterprise Management Console
Managed Objects
enterprise.local
Active Directory Change Reporter
Group Policy Change Reporter
Reports
Subscriptions
Sessions
2012.08.28 at 08:46:15, Tuesday
2012.08.28 at 08:57:00, Tuesday
2012.08.29 at 03:05:11, Wednesday
Exchange Change Reporter
Settings
Reports
Email Notifications
Audit Archive
Schedule
License
All Sessions
NetWrix
Systems Management and Compliance
Enterprise Management Console

Session: Wednesday, August 29, 2012 at 3:05:11 AM

Domain: enterprise.local

Status: Success

Type: Group Policy Change Reporter

Error Text: none

Click Run to generate report for this session

Run
Stop
View Change Summary for this session

The following information is provided:

Table 5: Session Details

Parameter	Description
Domain	Shows the name of the monitored domain.
Status	Shows the Session status. The values are: • Success • 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. For detailed instructions on how to do it, refer to Section 5.3.1 Viewing Change Summary for Sessions.

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 7.3 Configuring Audit Archive Settings.

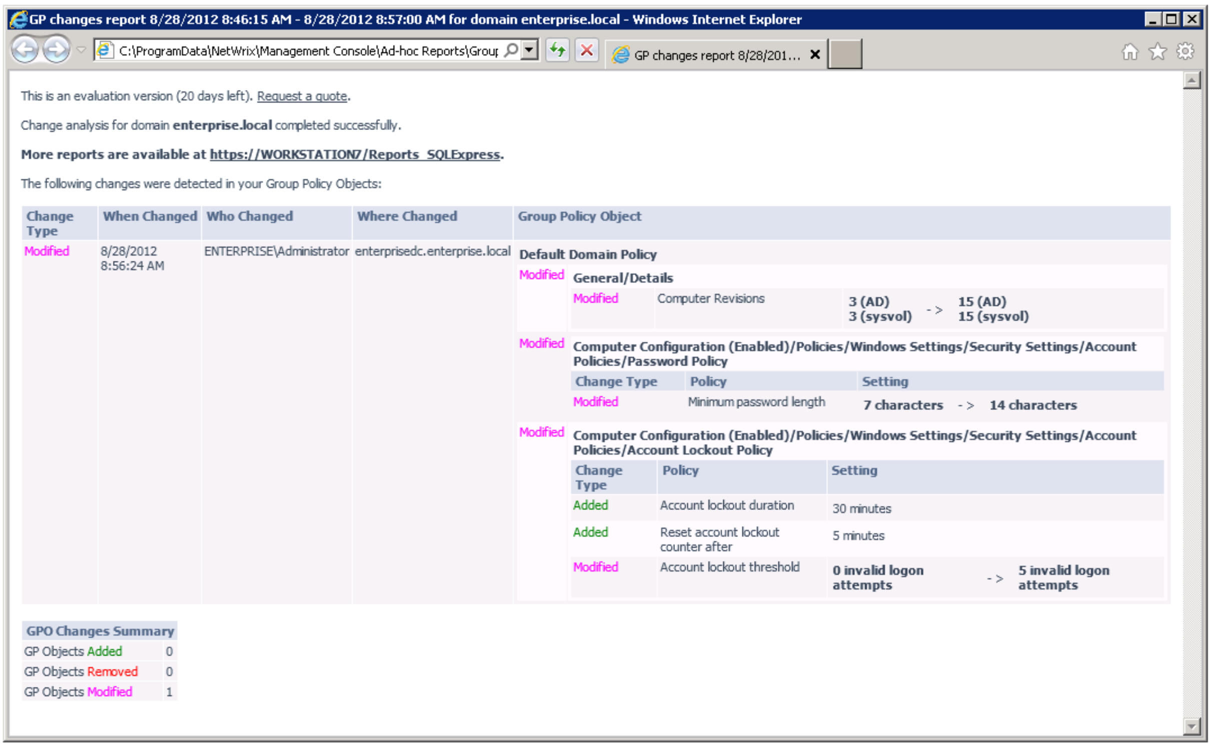
Copyright © 2012 NetWrix Corporation. All Rights Reserved

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 a Change Summary for.
2. In the right pane, click the **Run** button. 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 20: Web-based Change Summary



GP changes report 8/28/2012 8:46:15 AM - 8/28/2012 8:57:00 AM for domain enterprise.local - Windows Internet Explorer

C:\ProgramData\NetWrix\Management Console\Ad-hoc Reports\Grou

This is an evaluation version (20 days left). Request a quote.

Change analysis for domain **enterprise.local** completed successfully.

More reports are available at https://WORKSTATION7/Reports_SQLExpress.

The following changes were detected in your Group Policy Objects:

Change Type	When Changed	Who Changed	Where Changed	Group Policy Object
Modified	8/28/2012 8:56:24 AM	ENTERPRISE\Administrator	enterprisedc.enterprise.local	**Default Domain Policy**

Modified **General/Details**

Modified	Computer Revisions	**3 (AD)** **3 (sysvol)**	->	**15 (AD)** **15 (sysvol)**

Modified **Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Password Policy**

Change Type	Policy	Setting		
Modified	Minimum password length	**7 characters**	->	**14 characters**

Modified **Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Account Lockout Policy**

Change Type	Policy	Setting		
Added	Account lockout duration	30 minutes		
Added	Reset account lockout counter after	5 minutes		
Modified	Account lockout threshold	**0 invalid logon attempts**	->	**5 invalid logon attempts**

GPO Changes Summary	
GP Objects Added	0
GP Objects Removed	0
GP Objects Modified	1

Copyright © 2012 NetWrix Corporation. All Rights Reserved

6. REPORTS

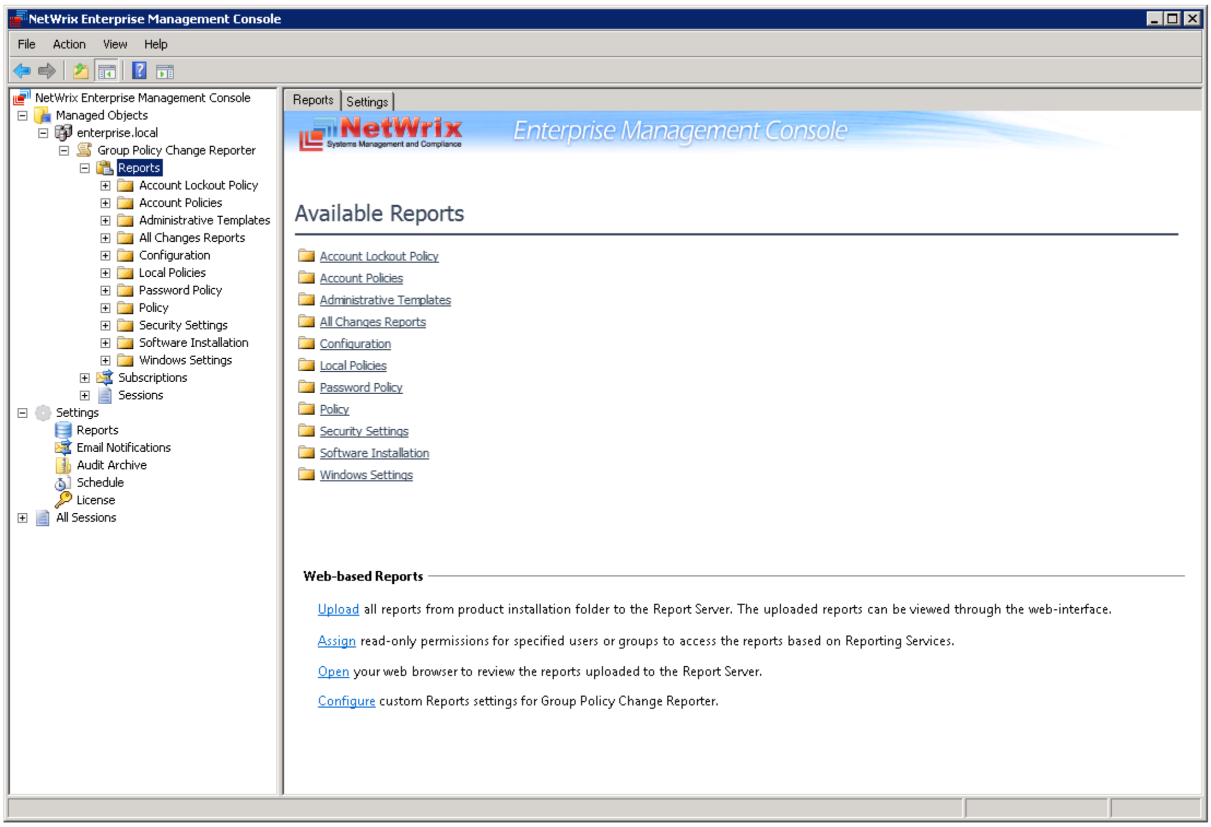
6.1. Reports Overview

NetWrix Group Policy 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.

For a full list of available reports, expand the Reports node under Managed Objects → <Managed_Object_name> → Group Policy Change Reporter:

Figure 21: The Reports Page



Available Reports

- Account Lockout Policy
- Account Policies
- Administrative Templates
- All Changes Reports
- Configuration
- Local Policies
- Password Policy
- Policy
- Security Settings
- Software Installation
- Windows Settings

Web-based Reports

Upload all reports from product installation folder to the Report Server. The uploaded reports can be viewed through the web-interface.

Assign read-only permissions for specified users or groups to access the reports based on Reporting Services.

Open your web browser to review the reports uploaded to the Report Server.

Configure custom Reports settings for Group Policy Change Reporter.

6.2. Configuring Reports

To configure the SSRS-based Reports, or modify the Reports settings for your Managed Object, perform the following operations:

- Configure SQL Server Settings
- Upload report templates to the SRS Server
- Import audit data from the Audit Archive to an SQL database
- Assigning Permissions to View Reports

Copyright © 2012 NetWrix Corporation. All Rights Reserved

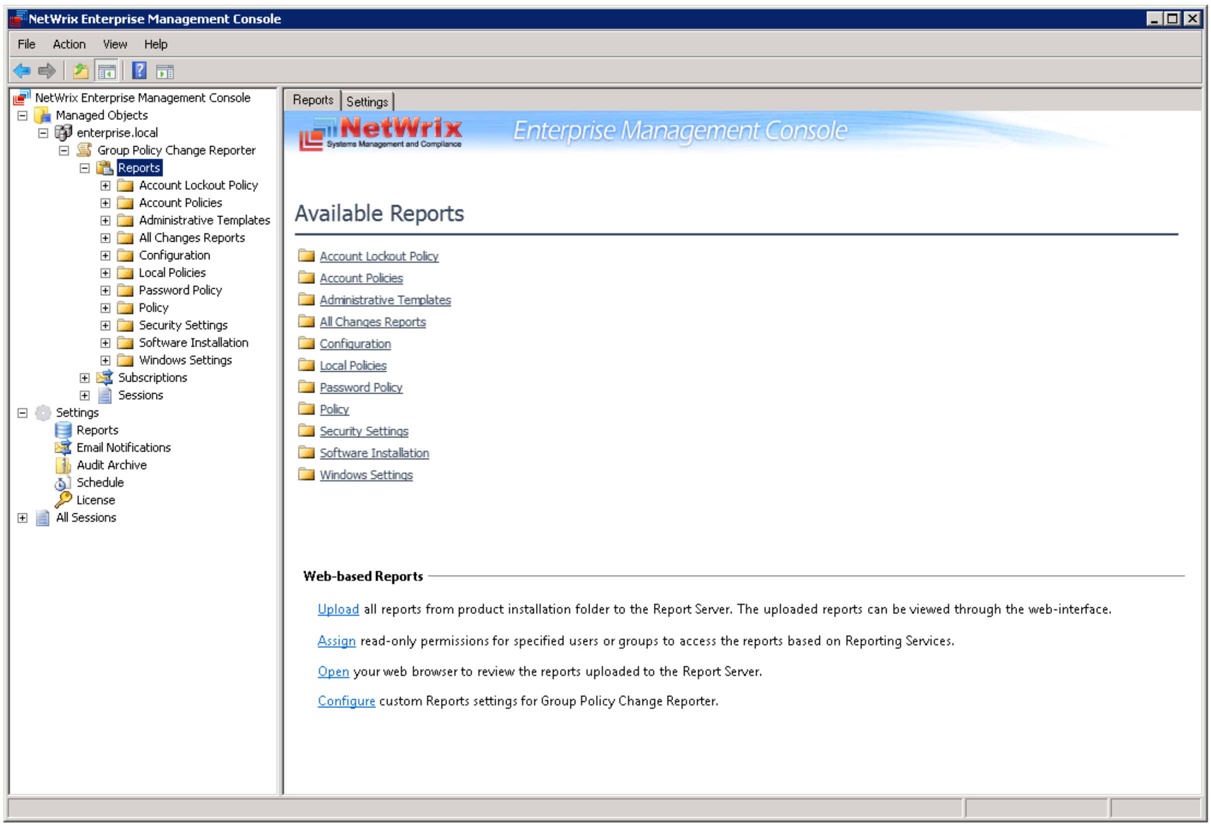
6.2.1. Configuring SQL Server Settings

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 SQL Server Settings

1. In NetWrix Enterprise Management Console, navigate to **Managed Object** → **<Managed_Object_name>** → **Group Policy Change Reporter** → **Reports**. The following page will be displayed:

Figure 22: The Reports Page



Available Reports

- Account Lockout Policy
- Account Policies
- Administrative Templates
- All Changes Reports
- Configuration
- Local Policies
- Password Policy
- Policy
- Security Settings
- Software Installation
- Windows Settings

Web-based Reports

Upload all reports from product installation folder to the Report Server. The uploaded reports can be viewed through the web-interface.

Assign read-only permissions for specified users or groups to access the reports based on Reporting Services.

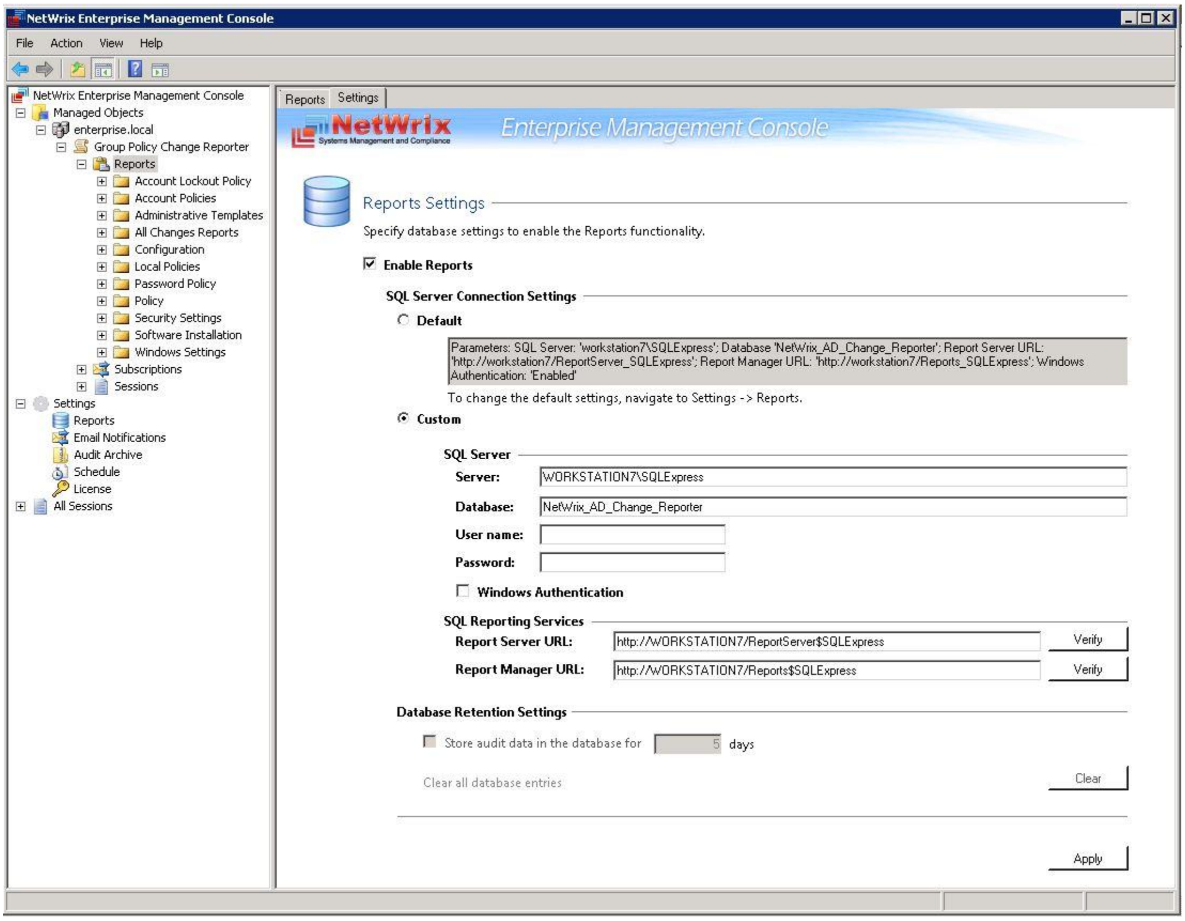
Open your web browser to review the reports uploaded to the Report Server.

Configure custom Reports settings for Group Policy Change Reporter.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

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

Figure 23: Reports Settings



Reports Settings

Specify database settings to enable the Reports functionality.

☑ Enable Reports

SQL Server Connection Settings

○ Default

Parameters: SQL Server: 'workstation7\SQLExpress'; Database 'NetWrix_AD_Change_Reporter'; Report Server URL: 'http://workstation7/ReportServer_SQLExpress'; Report Manager URL: 'http://workstation7/Reports_SQLExpress'; Windows Authentication: 'Enabled'

To change the default settings, navigate to Settings -> Reports.

● Custom

SQL Server

Server: WORKSTATION7\SQLExpress

Database: NetWrix_AD_Change_Reporter

User name:

Password:

☐ Windows Authentication

SQL Reporting Services

Report Server URL: http://WORKSTATION7/ReportServer$SQLExpress Verify

Report Manager URL: http://WORKSTATION7/Reports$SQLExpress Verify

Database Retention Settings

☐ Store audit data in the database for 5 days

Clear all database entries Clear

Apply

3. Specify or 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	Enter a user name for the SMTP authentication. This user must belong to the target database owner role.
Password	Enter a password for the SMTP authentication.
Windows Authentication	Select this check box if you want to use the default Data Processing Account (specified on Managed Object creation) to access the SQL database. Clear this box 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.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

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	This option is disabled in this product version.

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

Note: When you configure the Reports settings, an SQL database for audit data is created. If you skip the Reports configuration on the 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.

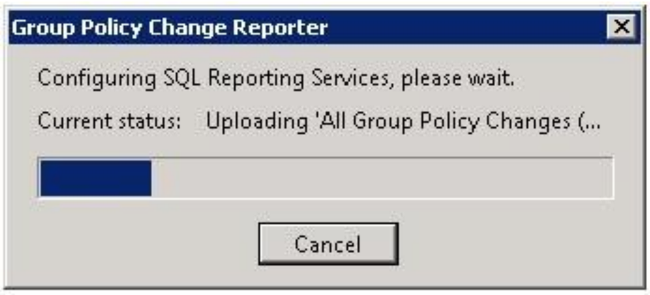
6.2.2. Uploading Report Templates to the Report Server

If you have not enabled the Reports feature when creating a Managed Object, and decided to enable it later, you need to upload the report templates to the Report Server. To upload the report templates, do the following:

Procedure 10. To upload report templates to the Report Server

- On the Reports page (see Figure 22: The 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 24: Uploading Report Templates



Group Policy Change Reporter

Configuring SQL Reporting Services, please wait.

Current status: Uploading 'All Group Policy Changes (...

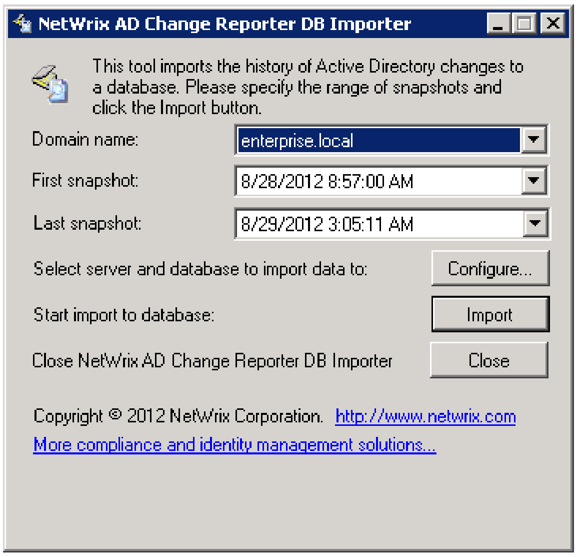
6.2.3. Importing Audit Data to SQL Database

If you have not enabled the Reports feature when creating a Managed Object, and decided 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 an 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 → Group Policy Change Reporter → Advanced Tools and select DB Importer. The DB Importer dialog will open:

Figure 25: NetWrix AD Change Reporter DB Importer



NetWrix AD Change Reporter DB Importer

This tool imports the history of Active Directory changes to a database. Please specify the range of snapshots and click the Import button.

Domain name: enterprise.local

First snapshot: 8/28/2012 8:57:00 AM

Last snapshot: 8/29/2012 3:05:11 AM

Select server and database to import data to: Configure...

Start import to database: Import

Close NetWrix AD Change Reporter DB Importer Close

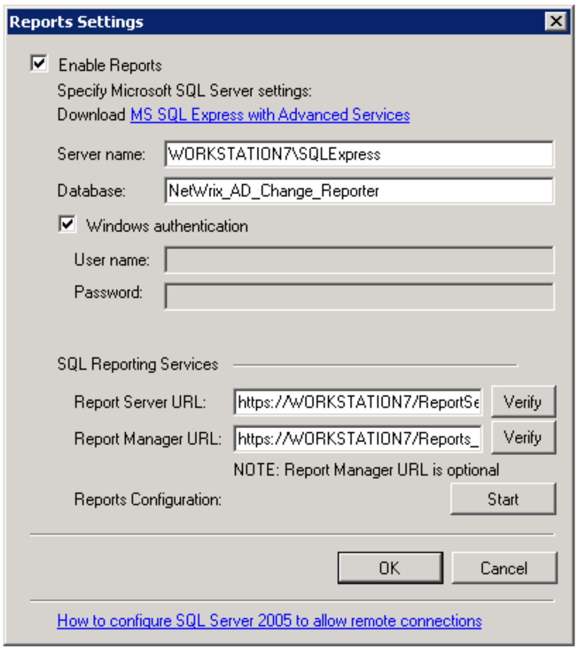
Copyright © 2012 NetWrix Corporation. http://www.netwrix.com

More compliance and identity management solutions...

2. Select your monitored domain in the **Domain name** menu 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 26: Reports Settings



Reports Settings

☑ Enable Reports

Specify Microsoft SQL Server settings:

Download MS SQL Express with Advanced Services

Server name: WORKSTATION7\SQLExpress

Database: NetWrix_AD_Change_Reporter

☑ Windows authentication

User name:

Password:

SQL Reporting Services

Report Server URL: https://WORKSTATION7/ReportSe Verify

Report Manager URL: https://WORKSTATION7/Reports_ Verify

NOTE: Report Manager URL is optional

Reports Configuration: Start

OK Cancel

How to configure SQL Server 2005 to allow remote connections

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.

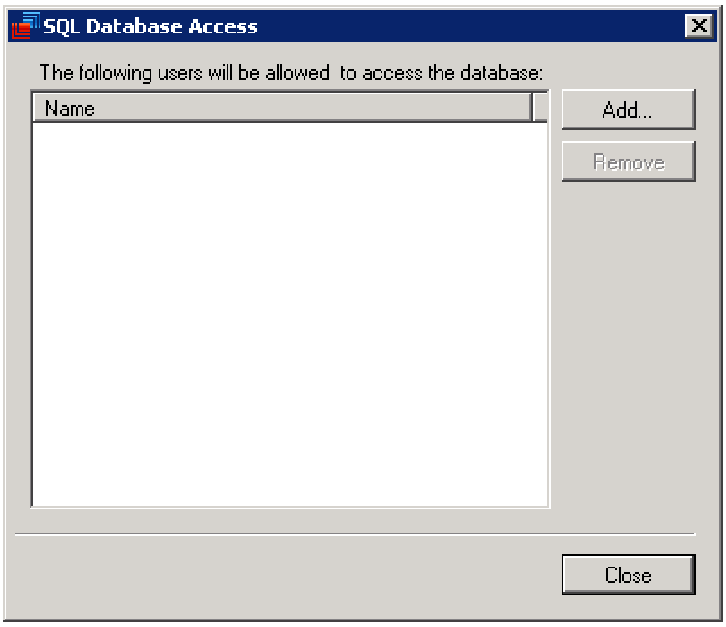
6.2.4. Assigning Permissions to View Reports

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 12. To assign permissions to view reports

1. On the Reports page (see Figure 22: The Reports Page), click **Assign** under **Web-based Reporting**. The following dialog will be displayed:

Figure 27: SQL Database Access



SQL Database Access

The following users will be allowed to access the database:

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 Group Policy 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

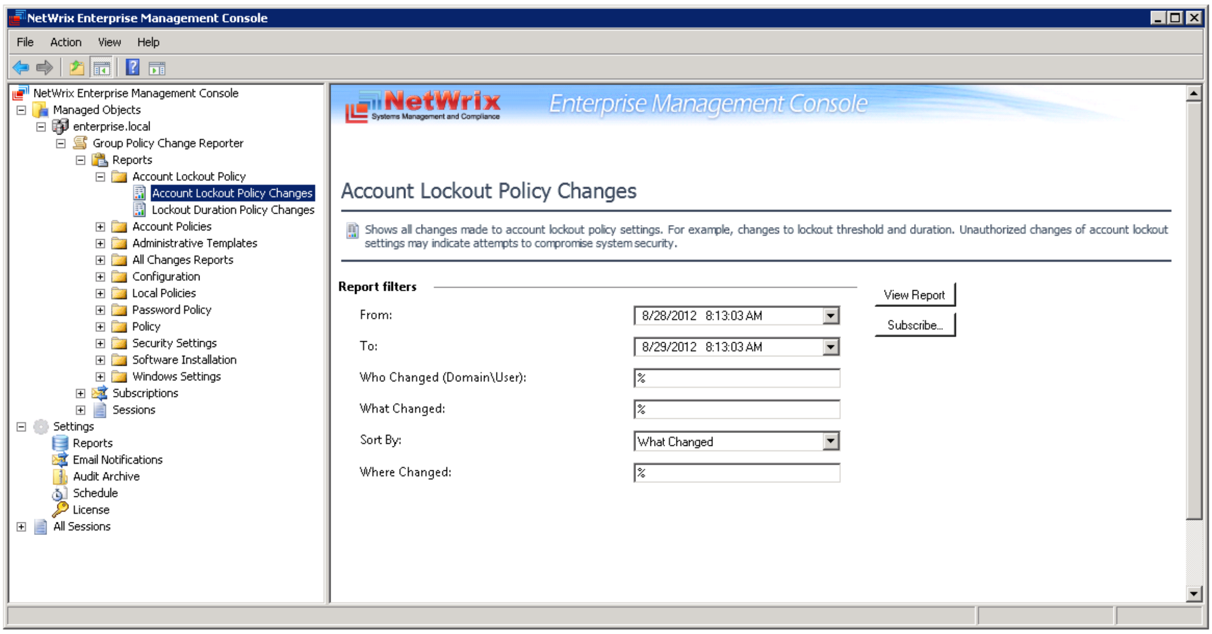
Procedure 13. To view a report in NetWrix Enterprise Management Console

1. In NetWrix Enterprise Management Console, navigate to Managed Objects → <Managed_Object_name> → Group Policy Change Reporter → Reports.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

2. Select a report from one of the folders. The Report Filters page will be displayed on the right:

Figure 28: The Report Filters Page



Account Lockout Policy Changes

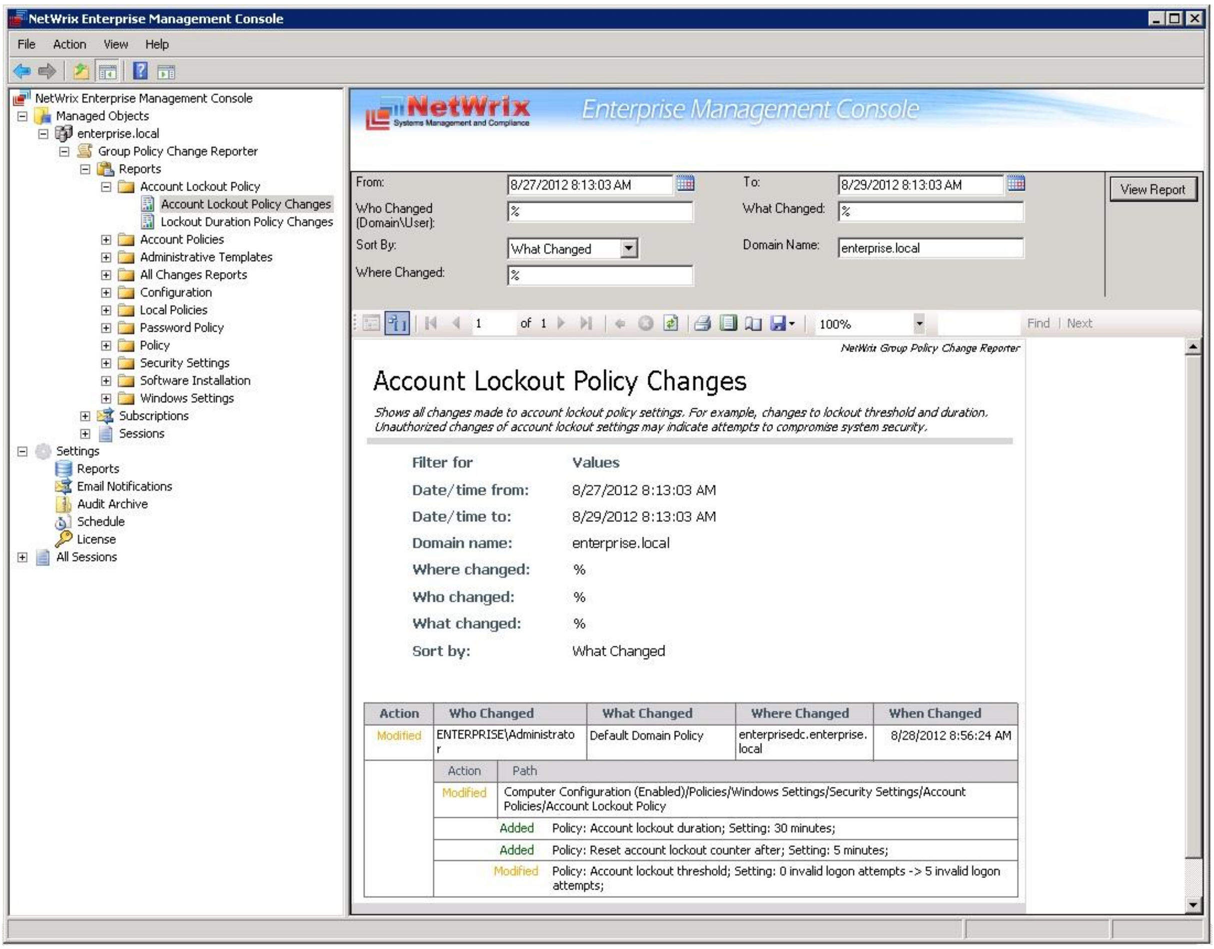
Shows all changes made to account lockout policy settings. For example, changes to lockout threshold and duration. Unauthorized changes of account lockout settings may indicate attempts to compromise system security.

Report filters

From:	8/28/2012 8:13:03 AM
To:	8/29/2012 8:13:03 AM
Who Changed (Domain\User):	%
What Changed:	%
Sort By:	What Changed
Where Changed:	%

3. Specify the report filters (a wildcard (%) can be used to replace any number of characters) and click the **View Report** button (**View Chart** for chart reports). The report will be displayed in the right pane:

Figure 29: The Account Lockout Policy Changes Report (Console)



From:	8/27/2012 8:13:03 AM	To:	8/29/2012 8:13:03 AM
Who Changed (Domain\User):	%	What Changed:	%
Sort By:	What Changed	Domain Name:	enterprise.local
Where Changed:	%		

Account Lockout Policy Changes

Shows all changes made to account lockout policy settings. For example, changes to lockout threshold and duration. Unauthorized changes of account lockout settings may indicate attempts to compromise system security.

Filter for	Values
Date/time from:	8/27/2012 8:13:03 AM
Date/time to:	8/29/2012 8:13:03 AM
Domain name:	enterprise.local
Where changed:	%
Who changed:	%
What changed:	%
Sort by:	What Changed

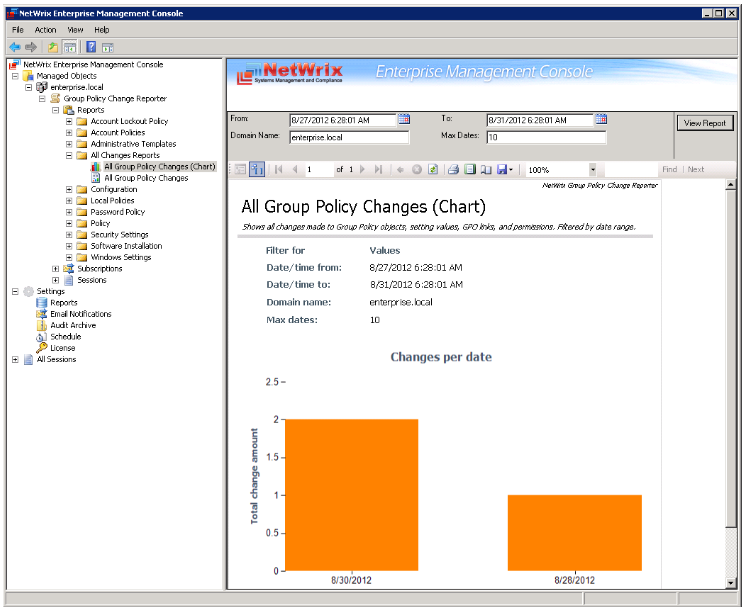
Action	Who Changed	What Changed	Where Changed	When Changed
Modified	ENTERPRISE\Administrator	Default Domain Policy	enterprisedc.enterprise.local	8/28/2012 8:56:24 AM

Action	Path
Modified	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Account Lockout Policy
Added	Policy: Account lockout duration; Setting: 30 minutes;
Added	Policy: Reset account lockout counter after; Setting: 5 minutes;
Modified	Policy: Account lockout threshold; Setting: 0 invalid logon attempts -> 5 invalid logon attempts;

Copyright © 2012 NetWrix Corporation. All Rights Reserved

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

Figure 30: All Group Policy Changes Chart (Chart)



From: 8/27/2012 6:28:01 AM
To: 8/31/2012 6:28:01 AM
Domain Name: enterprise.local
Max Dates: 10

All Group Policy Changes (Chart)

Shows all changes made to Group Policy objects, setting values, GPO links, and permissions. Filtered by date range.

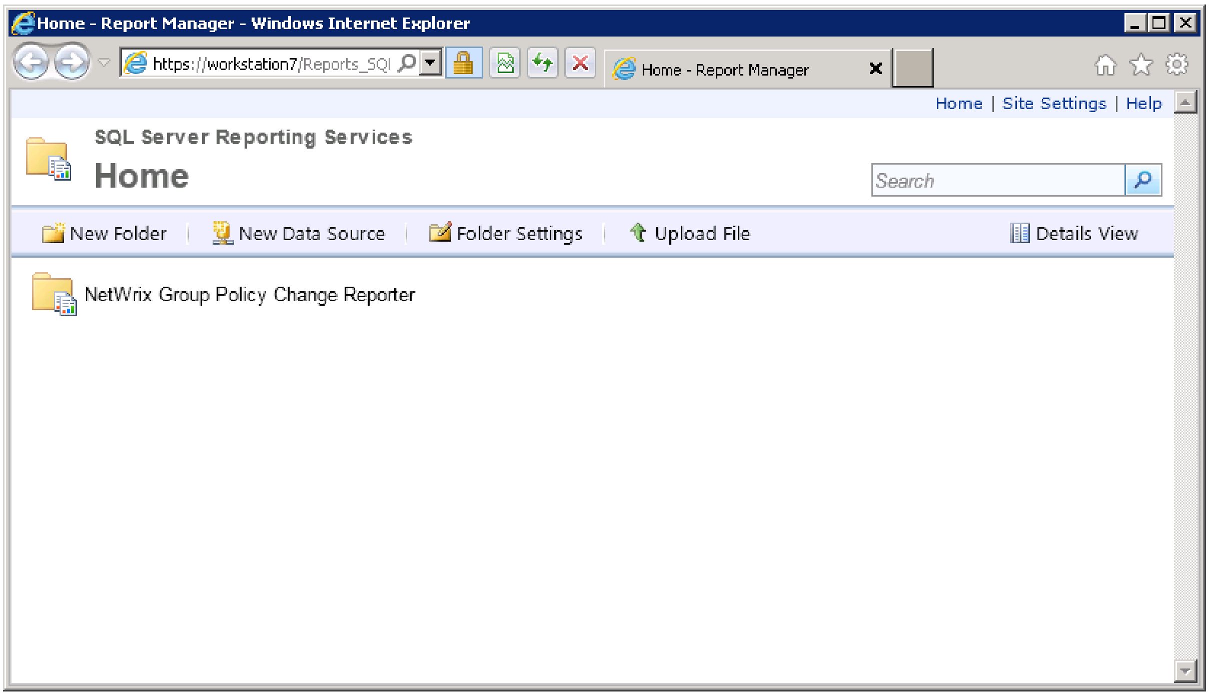
Filter for	Values
Date/time from:	8/27/2012 6:28:01 AM
Date/time to:	8/31/2012 6:28:01 AM
Domain name:	enterprise.local
Max dates:	10

6.3.2. Viewing Reports in a Web Browser

Procedure 14. To view a report in a web browser

1. Open a web browser and type in 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 22: The Reports Page](#)) and click **Open** under **Web-based Reports**. The following page will be displayed:

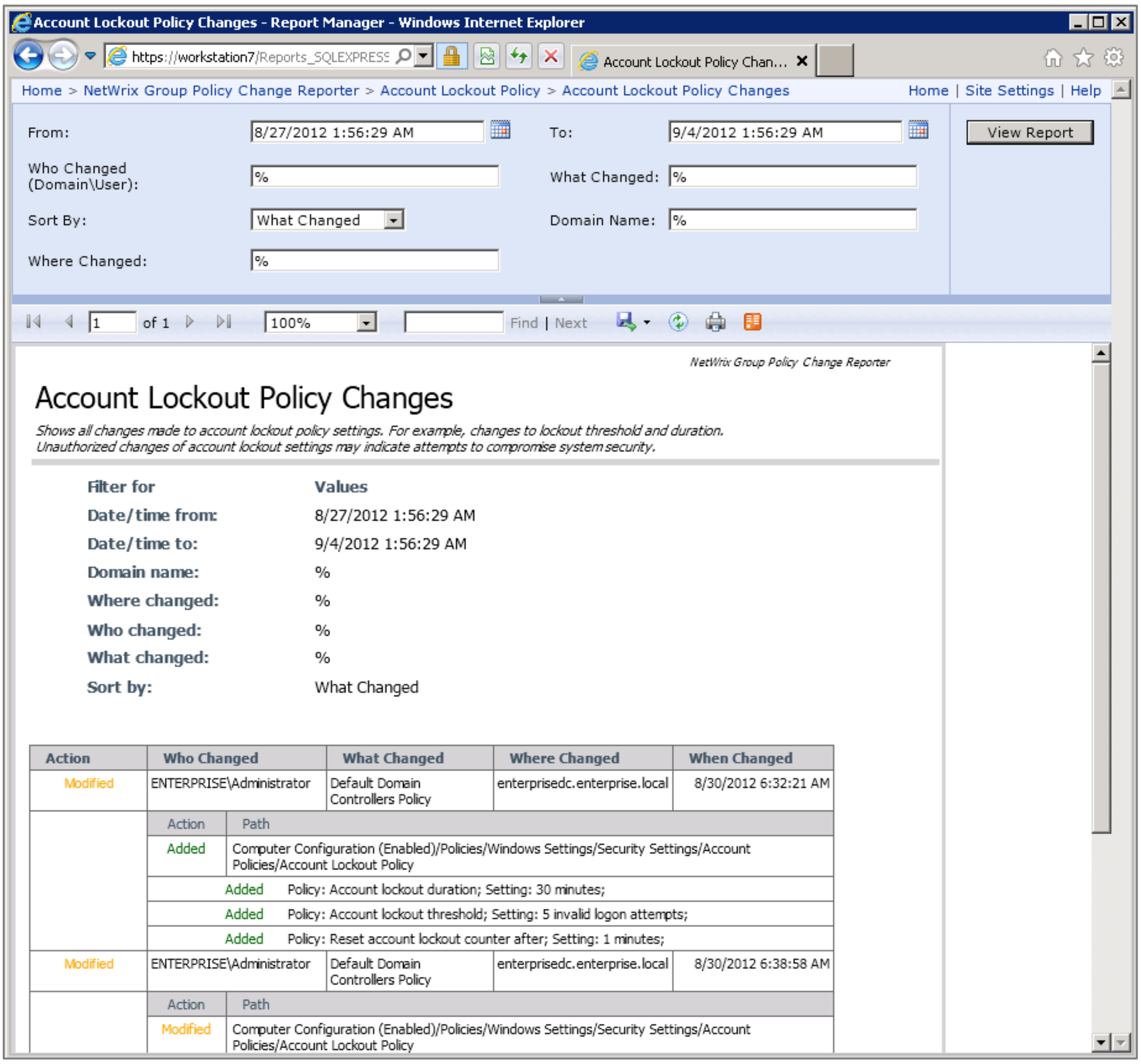
Figure 31: The SQL Server Reporting Services Page


Home - Report Manager - Windows Internet Explorer
https://workstation7/Reports_SQl
Home - Report Manager
Home | Site Settings | Help
SQL Server Reporting Services
Home
Search
New Folder
New Data Source
Folder Settings
Upload File
Details View
NetWrix Group Policy Change Reporter

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 Group Policy 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 report data: specify the required filter parameter on the top of the page and click the **View Report** button (**View Chart** for chart reports):

Figure 32: Account Lockout Policy Changes Report (Web Browser)


Account Lockout Policy Changes - Report Manager - Windows Internet Explorer
https://workstation7/Reports_SQLEXPRESS
Account Lockout Policy Chan...
Home > NetWrix Group Policy Change Reporter > Account Lockout Policy > Account Lockout Policy Changes
Home | Site Settings | Help
View Report
1 of 1
100%
Find | Next

From: 8/27/2012 1:56:29 AM

To: 9/4/2012 1:56:29 AM

Who Changed (Domain\User): %

What Changed: %

Sort By: What Changed

Domain Name: %

Where Changed: %

NetWrix Group Policy Change Reporter

Account Lockout Policy Changes

Shows all changes made to account lockout policy settings. For example, changes to lockout threshold and duration. Unauthorized changes of account lockout settings may indicate attempts to compromise system security.

Filter for	Values
Date/time from:	8/27/2012 1:56:29 AM
Date/time to:	9/4/2012 1:56:29 AM
Domain name:	%
Where changed:	%
Who changed:	%
What changed:	%
Sort by:	What Changed

Action	Who Changed	What Changed	Where Changed	When Changed
Modified	ENTERPRISE\Administrator	Default Domain Controllers Policy	enterprisedc.enterprise.local	8/30/2012 6:32:21 AM
	Action	Path		
	Added	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Account Lockout Policy		
		Added Policy: Account lockout duration; Setting: 30 minutes;		
		Added Policy: Account lockout threshold; Setting: 5 invalid logon attempts;		
		Added Policy: Reset account lockout counter after; Setting: 1 minutes;		
Modified	ENTERPRISE\Administrator	Default Domain Controllers Policy	enterprisedc.enterprise.local	8/30/2012 6:38:58 AM
	Action	Path		
	Modified	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Account Lockout Policy		

6.4. Configuring Report Subscriptions

In NetWrix Group Policy 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.

This section provides detailed instructions on how to:

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

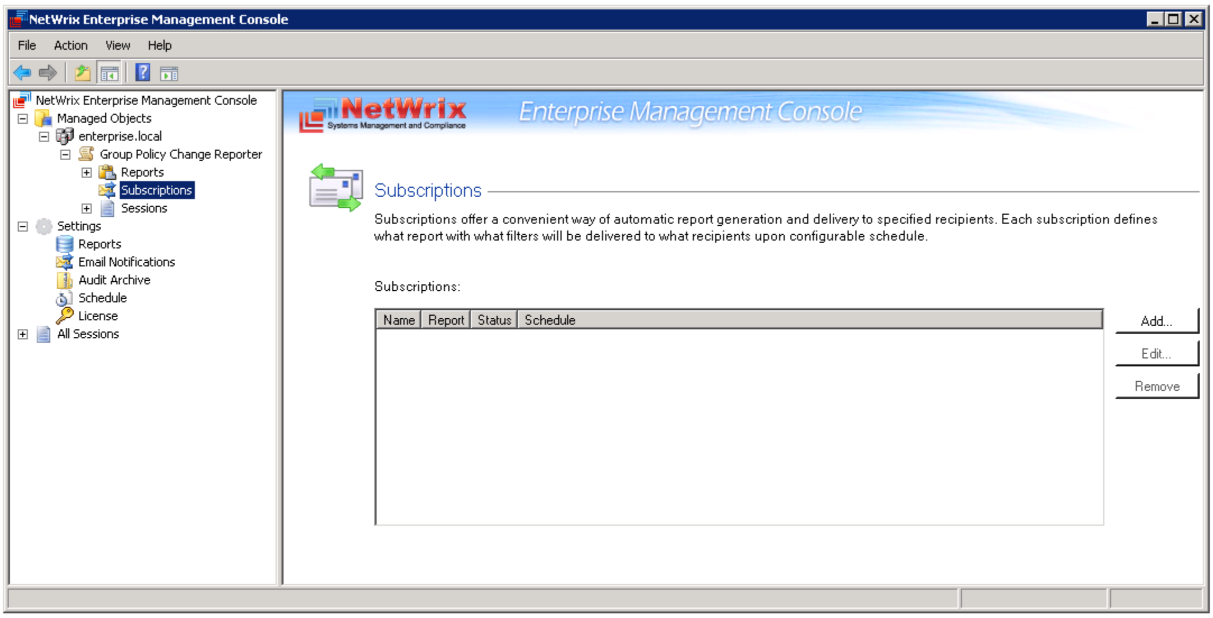
Copyright © 2012 NetWrix Corporation. All Rights Reserved

6.4.1. Creating a Subscription

Procedure 15. To create a Subscription

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

Figure 33: The Subscriptions Page



Subscriptions

Subscriptions offer a convenient way of automatic report generation and delivery to specified recipients. Each subscription defines what report with what filters will be delivered to what recipients upon configurable schedule.

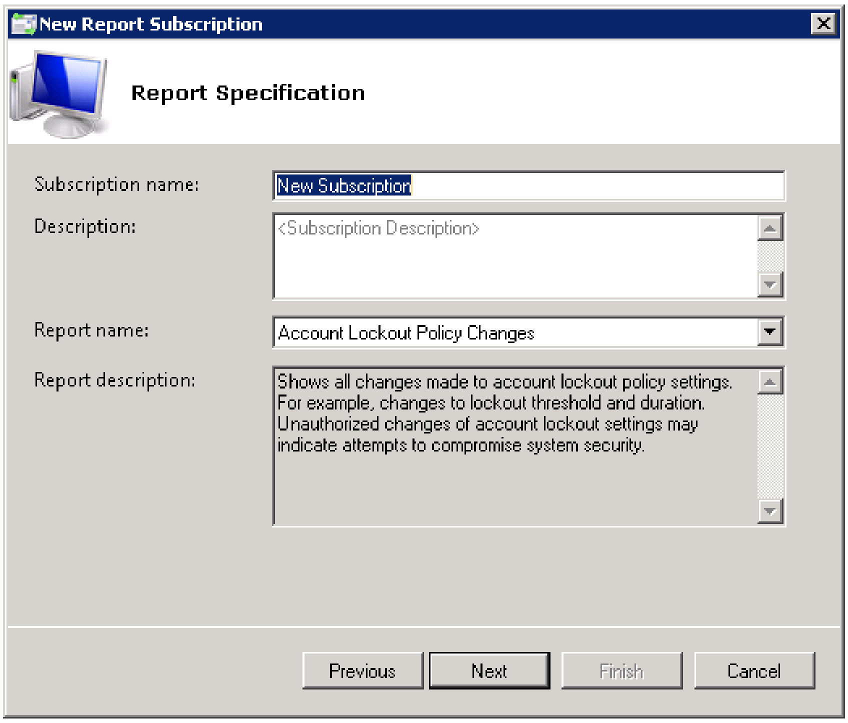
Subscriptions:

Name	Report	Status	Schedule

2. Click the **Add** button to start the Report Subscription wizard. You can also start the 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 34: New Report Subscription: Report Specification



Report Specification

Subscription name: New Subscription

Description: <Subscription Description>

Report name: Account Lockout Policy Changes

Report description: Shows all changes made to account lockout policy settings. For example, changes to lockout threshold and duration. Unauthorized changes of account lockout settings may indicate attempts to compromise system security.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

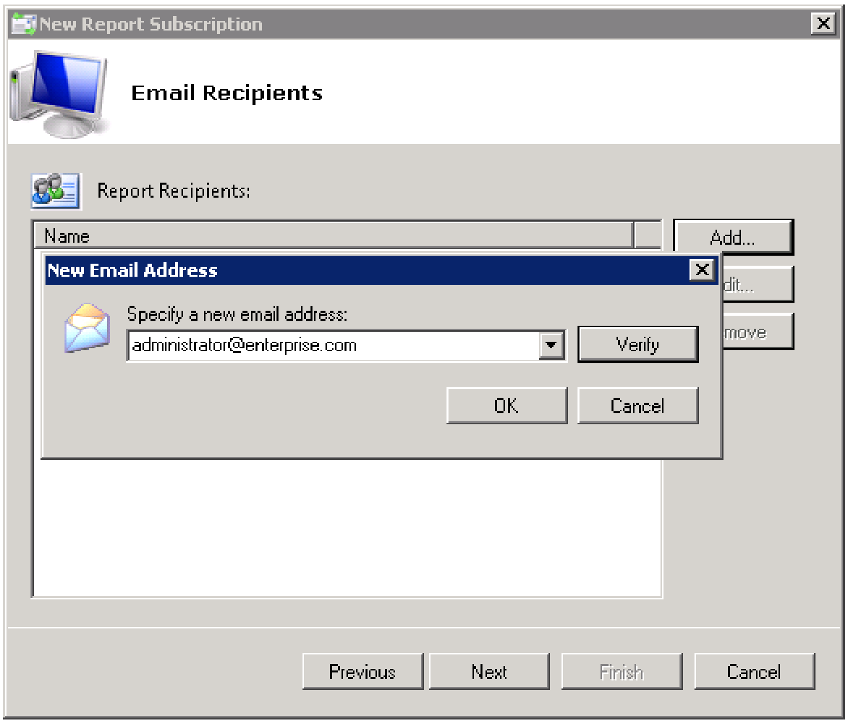
4. Specify the following parameters and click **Next**:

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 populated 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**.

Figure 35: New Report Subscription: Email Recipients



New Report Subscription

Email Recipients

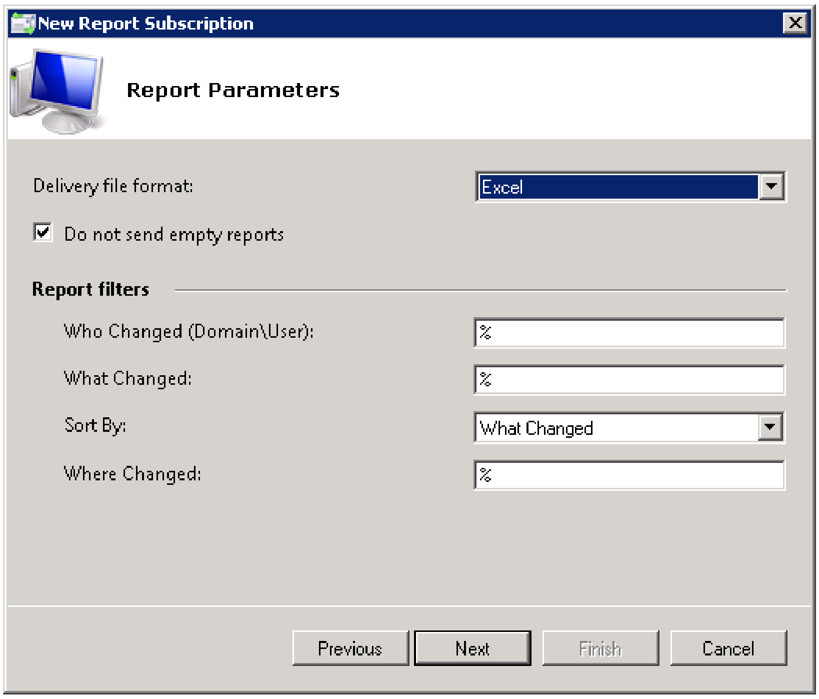
Report Recipients:

New Email Address

Specify a new email address: administrator@enterprise.com

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 when no changes occurred during the reporting period. Specify the report filters (which differ depending on the selected report) and click **Next**.

Figure 36: New Report Subscription: Report Parameters



New Report Subscription

Report Parameters

Delivery file format: Excel

☑ Do not send empty reports

Report filters

Who Changed (Domain\User): %

What Changed: %

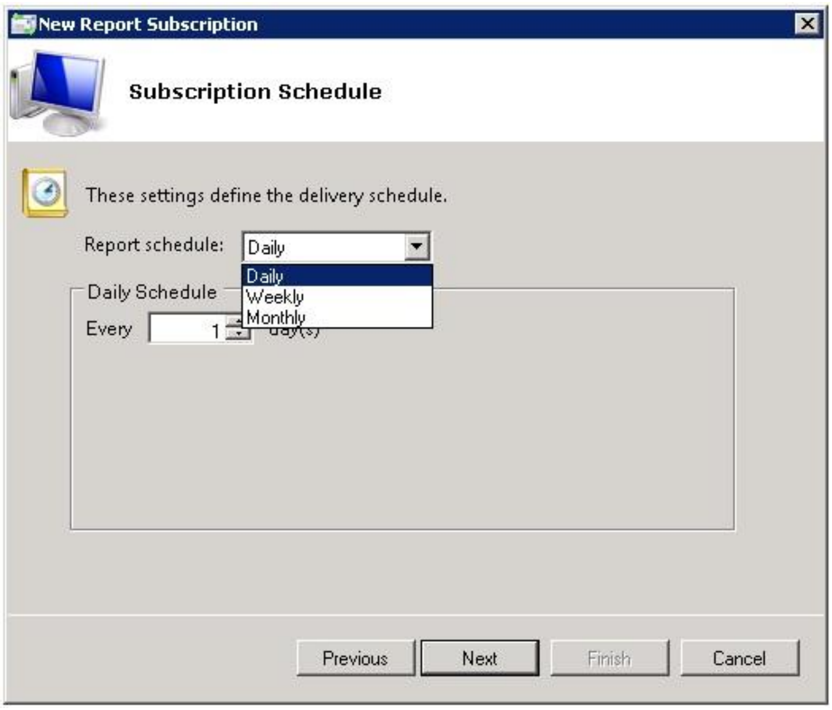
Sort By: What Changed

Where Changed: %

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 37: New Report Subscription Wizard: Subscription Schedule



New Report Subscription

Subscription Schedule

These settings define the delivery schedule.

Report schedule: Daily

Daily Schedule

Every 1 day(s)

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.

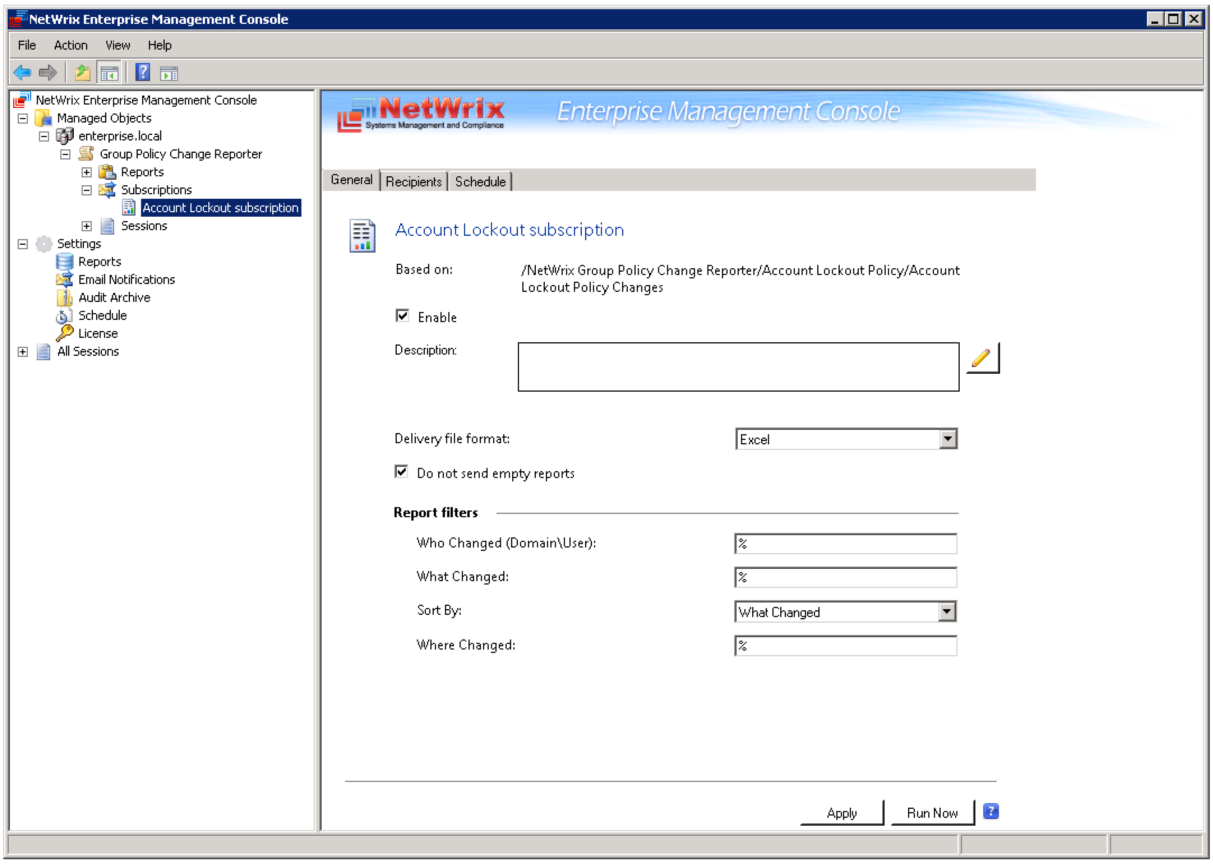
Copyright © 2012 NetWrix Corporation. All Rights Reserved

6.4.2. Modifying a Subscription

Procedure 16. To modify a Subscription

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

Figure 38: The Subscription Page



Account Lockout subscription

Based on: /NetWrix Group Policy Change Reporter/Account Lockout Policy/Account Lockout Policy Changes

☑ Enable

Description:

Delivery file format: Excel

☑ Do not send empty reports

Report filters

Who Changed (Domain\User): %

What Changed: %

Sort By: What Changed

Where Changed: %

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

6.4.3. Forcing on-Demand Report Delivery

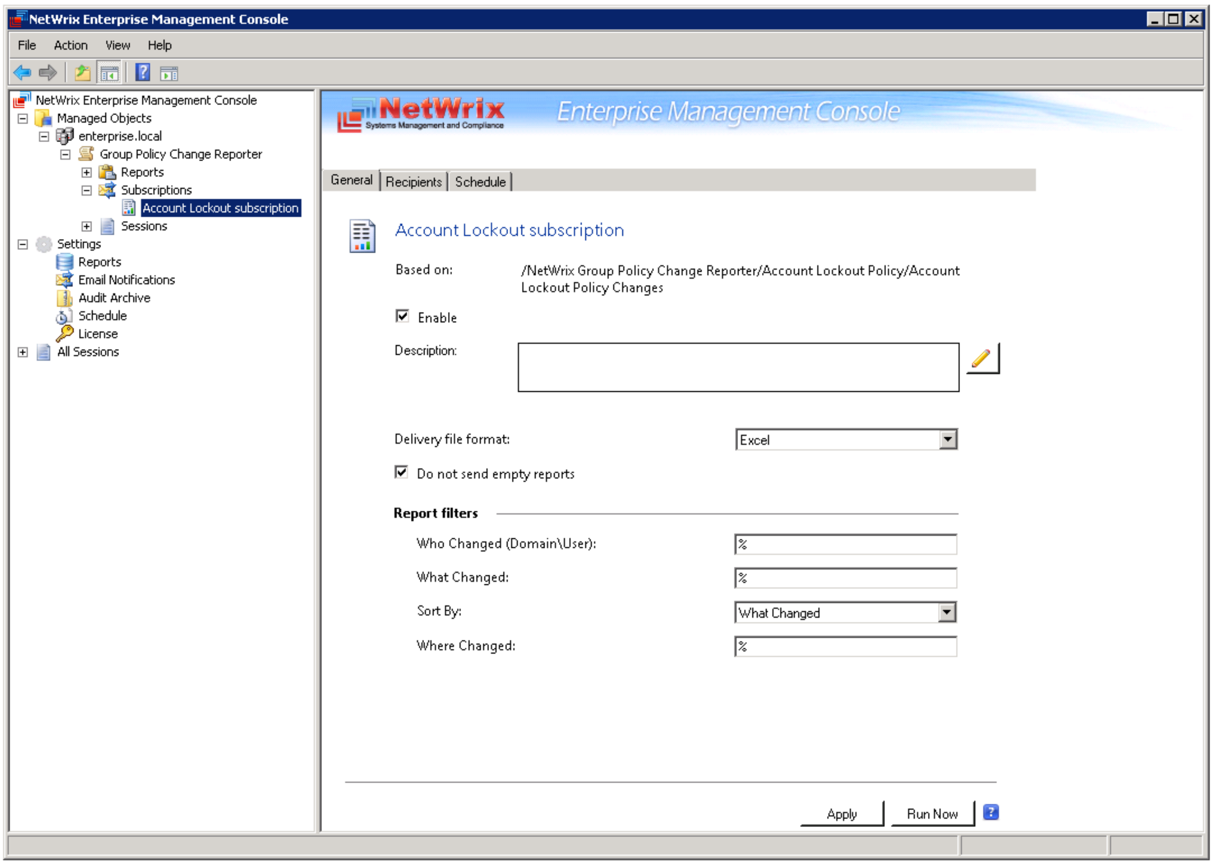
You can force an on-demand delivery of any report that you have configured a subscription for.

Procedure 17. To force on-demand report delivery

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<Managed_Object_name>** → **Group Policy Change Reporter** → **Subscriptions** node and select the Subscription for the report that you want to generate and send.
2. On the report Subscription page, click **Run Now**:

Copyright © 2012 NetWrix Corporation. All Rights Reserved

Figure 39: Report Subscription Page



NetWrix Enterprise Management Console
File Action View Help
NetWrix Enterprise Management Console
Managed Objects
enterprise.local
Group Policy Change Reporter
Reports
Subscriptions
Account Lockout subscription
Sessions
Settings
Reports
Email Notifications
Audit Archive
Schedule
License
All Sessions
NetWrix Systems Management and Compliance
Enterprise Management Console
General
Recipients
Schedule
Apply
Run Now

Account Lockout subscription

Based on: /NetWrix Group Policy Change Reporter/Account Lockout Policy/Account Lockout Policy Changes

☑ Enable

Description:

Delivery file format: Excel

☑ Do not send empty reports

Report filters

Who Changed (Domain\User): %

What Changed: %

Sort By: What Changed

Where Changed: %

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).

Copyright © 2012 NetWrix Corporation. All Rights Reserved

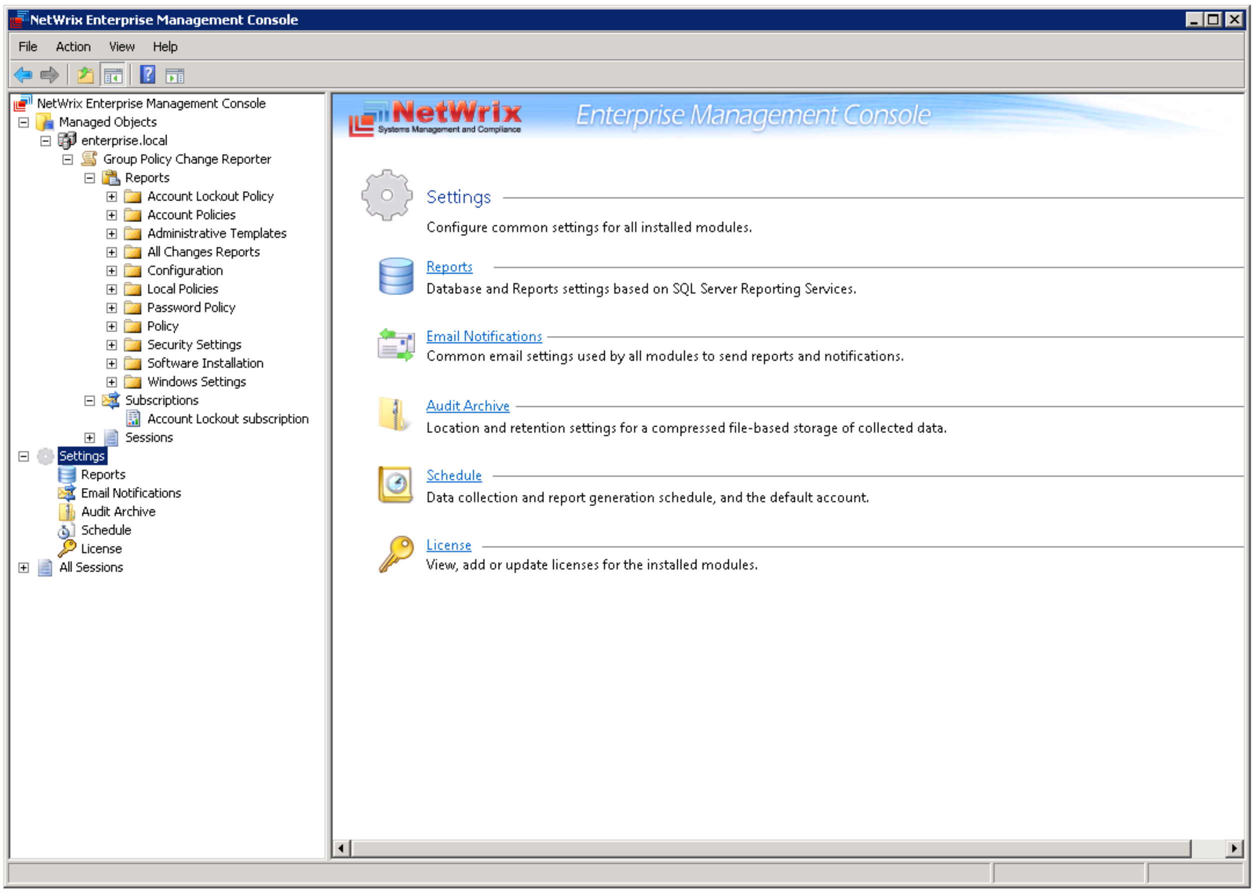
7. Configuring Global Settings

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 40: The Settings Page



Settings
Configure common settings for all installed modules.

Reports
Database and Reports settings based on SQL Server Reporting Services.

Email Notifications
Common email settings used by all modules to send reports and notifications.

Audit Archive
Location and retention settings for a compressed file-based storage of collected data.

Schedule
Data collection and report generation schedule, and the default account.

License
View, add or update licenses for the installed modules.

The following global settings can be configured:

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

Copyright © 2012 NetWrix Corporation. All Rights Reserved

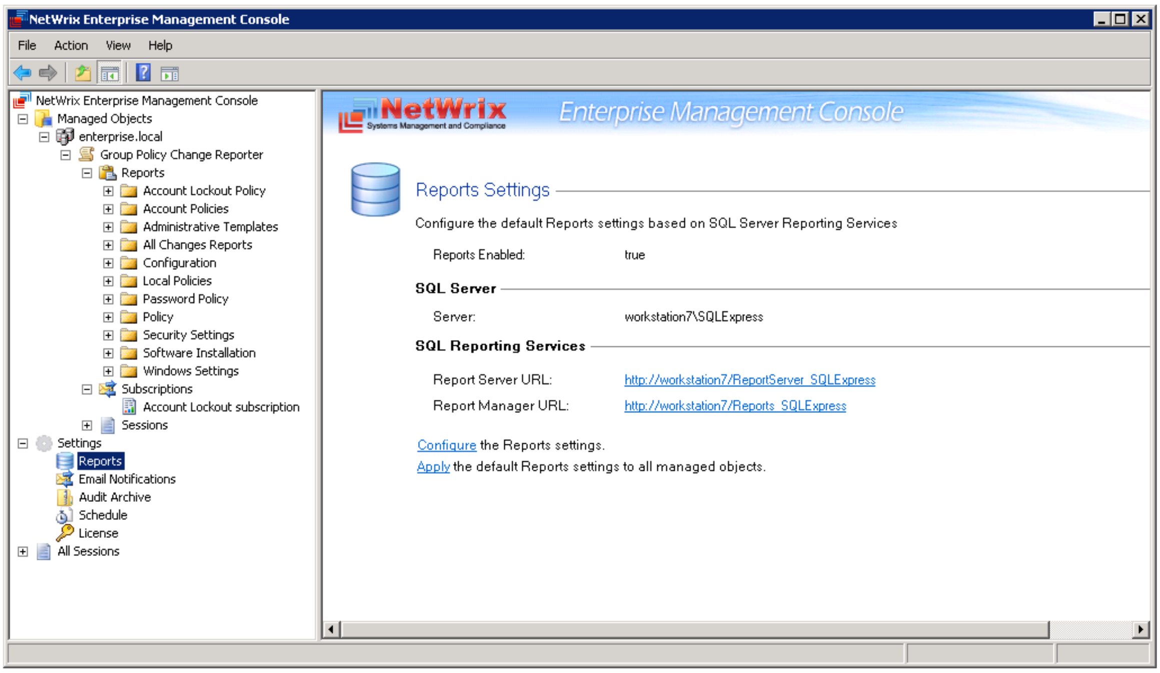
7.1. Configuring the Reports Settings

The **Reports** option allows configuring the SQL Server and Report Server settings.

Procedure 18. To configure the Reports settings

1. In NetWrix Enterprise Management Console, navigate to **Settings** → **Reports**. Alternatively, you can click **Reports** in the **Settings** page. The following page will be displayed showing the current Reports settings:

Figure 41: Settings: Reports



Reports Settings

Configure the default Reports settings based on SQL Server Reporting Services

Reports Enabled: true

SQL Server

Server: workstation7\SQLExpress

SQL Reporting Services

Report Server URL: http://workstation7/ReportServer_SQLExpress

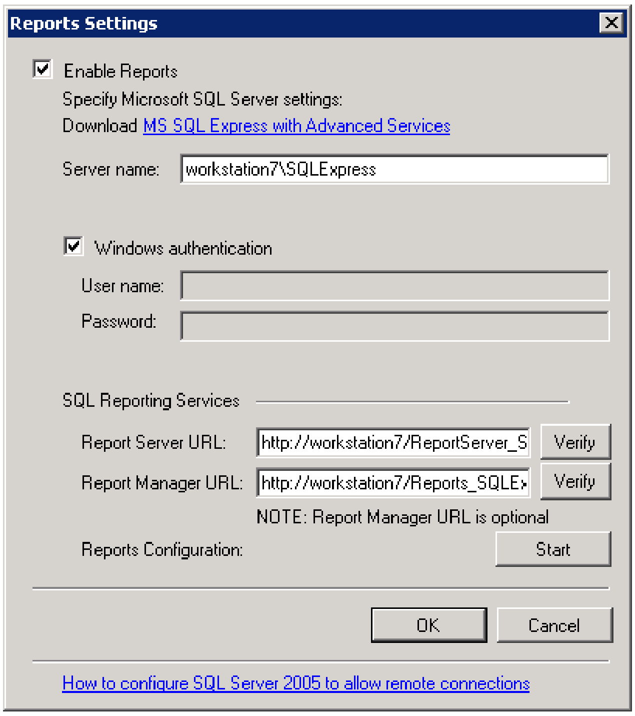
Report Manager URL: http://workstation7/Reports_SQLExpress

Configure the Reports settings.

Apply the default Reports settings to all managed objects.

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

Figure 42: Reports Settings



☑ Enable Reports

Specify Microsoft SQL Server settings:

Download MS SQL Express with Advanced Services

Server name: workstation7\SQLExpress

☑ Windows authentication

User name:

Password:

SQL Reporting Services

Report Server URL: http://workstation7/ReportServer_S

Report Manager URL: http://workstation7/Reports_SQLE›

NOTE: Report Manager URL is optional

Reports Configuration:

How to configure SQL Server 2005 to allow remote connections

Copyright © 2012 NetWrix Corporation. All Rights Reserved

3. Specify or modify the following settings:

Table 8: Reports Settings

Parameter	Description
Enable Reports	Select this check box 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 box if you want to use the Data Processing Account you specified on the Managed Object creation to access the SQL database. Clear the box to use the SQL Server authentication.
User name:	Specify a user name for the SQL Server authentication. **NOTE:** This user 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.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

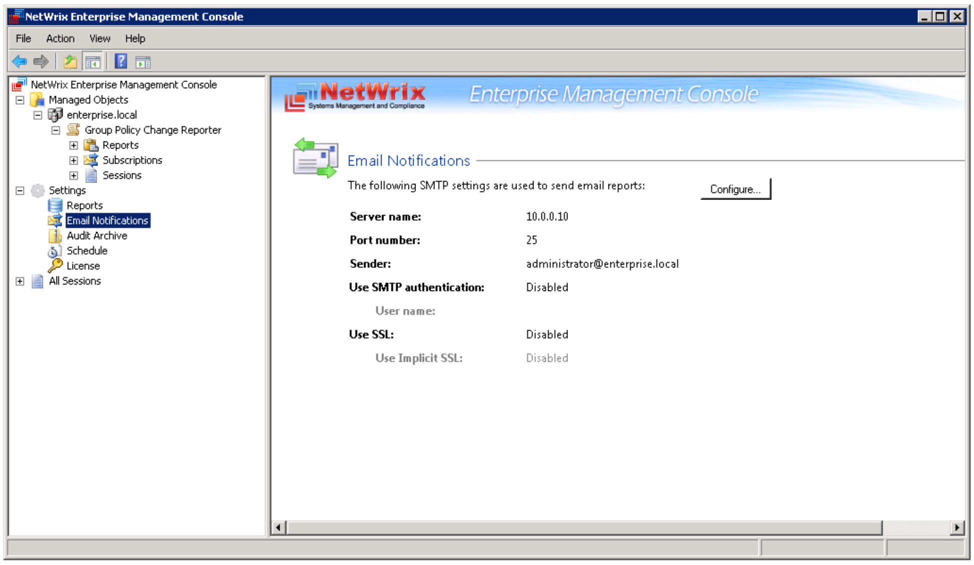
7.2. Configuring the Email Notifications Settings

The **Email Notifications** option allows configuring the SMTP settings used to deliver Change Summaries and Reports.

Procedure 19. To configure the email notifications settings

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

Figure 43: Settings: Email Notifications



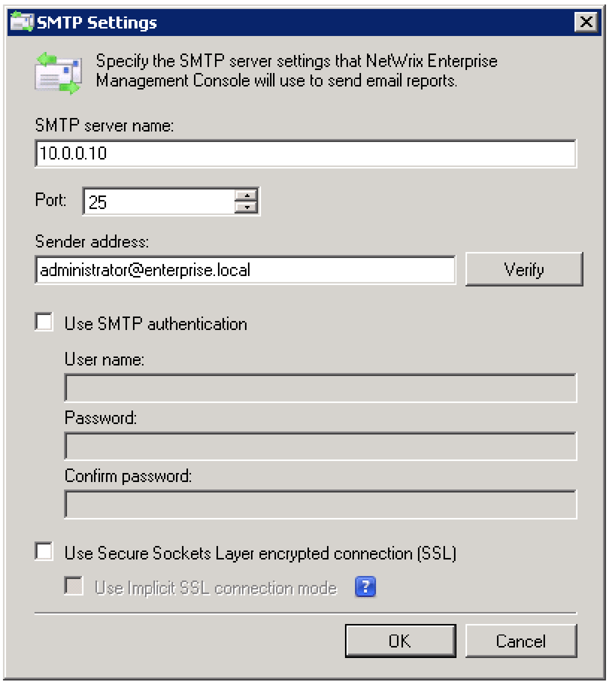
Email Notifications

The following SMTP settings are used to send email reports:

Server name:	10.0.0.10
Port number:	25
Sender:	administrator@enterprise.local
Use SMTP authentication:	Disabled
User name:	
Use SSL:	Disabled
Use Implicit SSL:	Disabled

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

Figure 44: SMTP Settings



Specify the SMTP server settings that NetWrix Enterprise Management Console will use to send email reports.

SMTP server name: 10.0.0.10

Port: 25

Sender address: administrator@enterprise.local

☐ Use SMTP authentication

User name:

Password:

Confirm password:

☐ Use Secure Sockets Layer encrypted connection (SSL)

☐ Use Implicit SSL connection mode

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

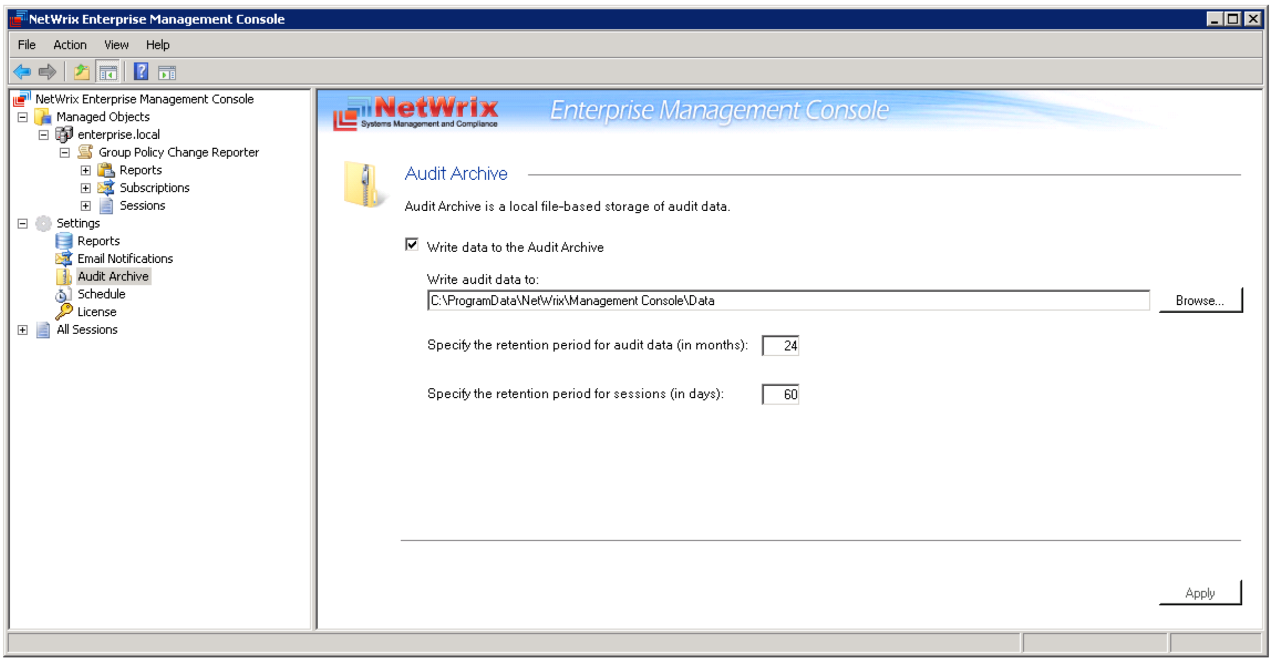
7.3. Configuring Audit Archive Settings

The **Audit Archive** option allows configuring the settings for the local repository of audit data.

Procedure 20. To configure the Audit Archive settings

1. In NetWrix Enterprise Management Console, navigate to **Settings** → **Audit Archive**. Alternatively, you can click **Audit Archive** in the Settings page. The following page will be displayed showing the current Audit Archive settings:

Figure 45: Settings: Audit Archive



Audit Archive

Audit Archive is a local file-based storage of audit data.

☑ Write data to the Audit Archive

Write audit data to: C:\ProgramData\NetWrix\Management Console\Data

Specify the retention period for audit data (in months): 24

Specify the retention period for sessions (in days): 60

2. You can modify the following settings:

Table 9: 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 (that is 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, because if the audit data is not written locally, it will not be imported to the SQL database and will be unavailable for reports.

7.4. Configuring Data Processing Account Setting

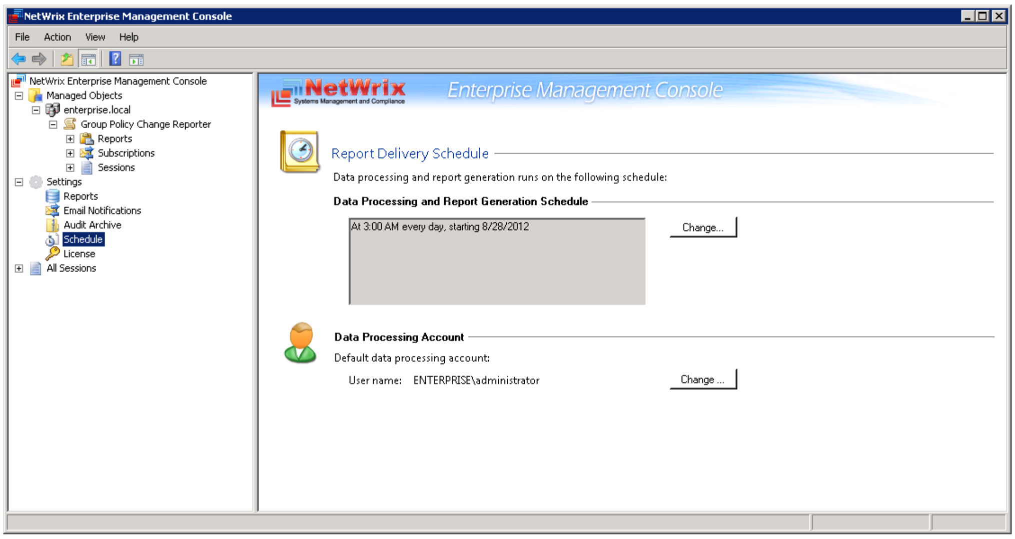
The **Schedule** option allows modifying the default settings for Data Processing Account. To modify these settings, do the following:

Copyright © 2012 NetWrix Corporation. All Rights Reserved

Procedure 21. To modify Data Processing Account settings

1. In NetWrix Enterprise Management Console, navigate to **Settings** → **Schedule**. Alternatively, you can click **Schedule** in the Settings page. The following page will be displayed showing the current data processing settings:

Figure 46: Settings: Schedule


NetWrix Enterprise Management Console
File
Action
View
Help
NetWrix Enterprise Management Console
Managed Objects
enterprise.local
Group Policy Change Reporter
Reports
Subscriptions
Sessions
Settings
Reports
Email Notifications
Audit Archive
Schedule
License
All Sessions
NetWrix
Systems Management and Compliance
Enterprise Management Console

Report Delivery Schedule

Data processing and report generation runs on the following schedule:

Data Processing and Report Generation Schedule

At 3:00 AM every day, starting 8/28/2012

Change...

Data Processing Account

Default data processing account:

User name: ENTERPRISE\administrator

Change ...

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

Note: The **Data Processing and Report Generation Schedule** setting is inapplicable to NetWrix Group Policy Change Reporter.

7.5. Configuring License Settings

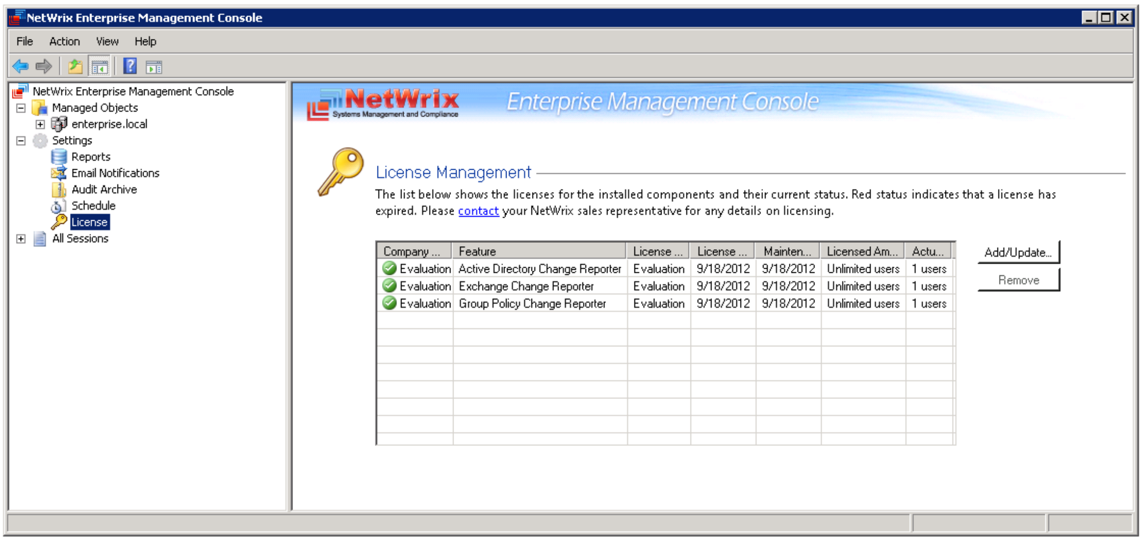
The **License** option allows viewing your current licenses for the installed NetWrix products, updating them and adding new licenses.

Procedure 22. To configure licenses

1. In NetWrix Enterprise Management Console, navigate to **Settings** → **License**. Alternatively, you can click **License** in the Settings page. The following page will be displayed showing the list of your current licenses:

Copyright © 2012 NetWrix Corporation. All Rights Reserved

Figure 47: Settings: License


NetWrix Enterprise Management Console
File
Action
View
Help
NetWrix Enterprise Management Console
Managed Objects
enterprise.local
Settings
Reports
Email Notifications
Audit Archive
Schedule
License
All Sessions
NetWrix
Systems Management and Compliance
Enterprise Management Console

License Management

The list below shows the licenses for the installed components and their current status. Red status indicates that a license has expired. Please contact your NetWrix sales representative for any details on licensing.

Company ...	Feature	License ...	License ...	Mainten...	Licensed Am...	Actu...
✓ Evaluation	Active Directory Change Reporter	Evaluation	9/18/2012	9/18/2012	Unlimited users	1 users
✓ Evaluation	Exchange Change Reporter	Evaluation	9/18/2012	9/18/2012	Unlimited users	1 users
✓ Evaluation	Group Policy Change Reporter	Evaluation	9/18/2012	9/18/2012	Unlimited users	1 users

2. The following options are available:

- 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 Group Policy Change Reporter is a 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.

8. Additional Configuration

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

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

8.1. Enabling Integration with Third-Party SIEM Solutions

If your organization is already using a third-party SIEM solution, NetWrix Group Policy 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 Group Policy 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 other.

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.

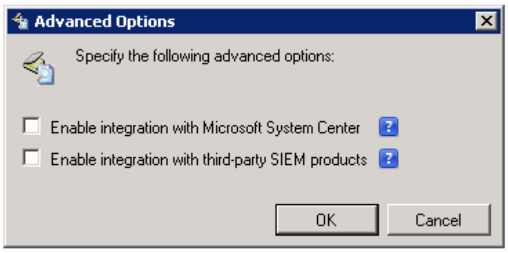
If you are using Microsoft SCOM and want to integrate it with NetWrix Group Policy Change Reporter, you need to install NetWrix Group Policy Change Reporter SCOM Management Pack, which is a solution that captures events written by NetWrix Group Policy Change Reporter into the dedicated event log, and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

To enable integration with SIEM systems, do the following:

Procedure 23. To enable integration with third-party SIEM solutions

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

Figure 48: The Advanced Options Dialog



Advanced Options

Specify the following advanced options:

☐ Enable integration with Microsoft System Center

☐ Enable integration with third-party SIEM products

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.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

8.2. Excluding/Including Data Types From/in Reports

You can fine-tune NetWrix Group Policy Change Reporter by specifying various data types that you want to exclude from the 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 description, syntax and examples. One entry per line is accepted.

Table 10: NetWrix Group Policy Change Reporter Configuration Files

File Name	Description	Syntax	Example
omitobjlist_gp.txt	Contains a list of the Group Policy Object (GPO) names to be excluded from change reports.	<object name> **NOTE**: A wildcard (*) can be used to replace any number of characters.	To exclude changes to the Default Domain Policy GPO, add the following line: `Default Domain Policy`
omitproplist_gp.txt	Contains a list of the Group Policy Object settings to be excluded from change reports.	<settingname> **NOTE**: A wildcard (*) can be used to replace any number of characters.	To exclude data on changes made to the Maximum password length setting, add the following line: `Maximum password length`
omituserlist_gp	Contains a list of user names to exclude particular users from change reports.	<domain\user> **NOTE**: A wildcard (*) can be used to replace any number of characters.	To exclude changes made by the user "usertest" in the domain "domaintest", add the following line: domaintest\usertest

Copyright © 2012 NetWrix Corporation. All Rights Reserved

9. RESTORING GROUP POLICY OBJECTS

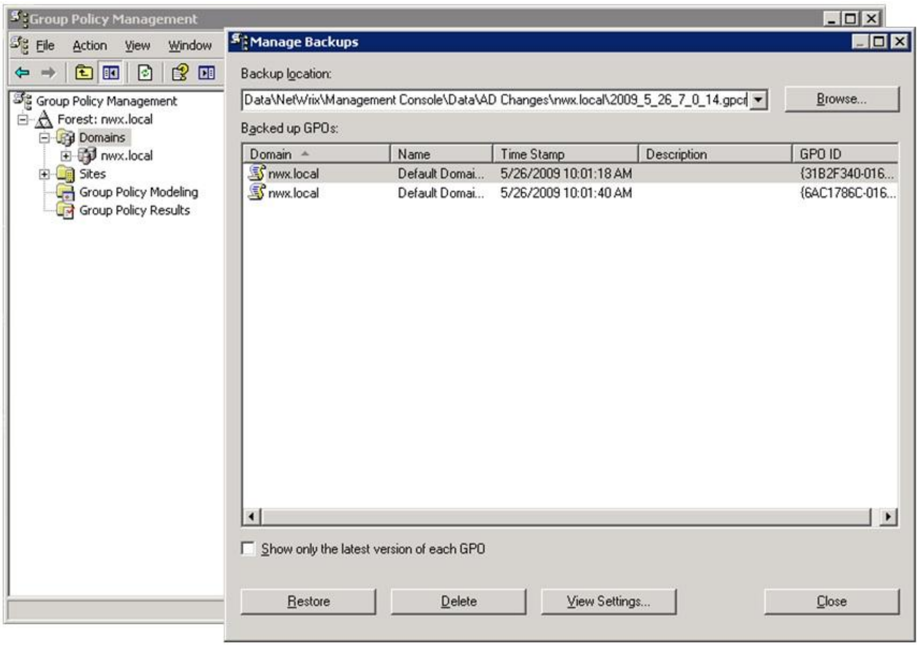
With NetWrix Group Policy Change Reporter, you can restore your Group Policy objects via the backup files saved by the product. The backups are stored in the folder with snapshots and event log information, the default path is: %ProgramData%\NetWrix\Management Console\Data\AD Changes\<domain_name>.

You can use this feature after at least one data collection task has run.

Procedure 24. To restore Group Policy objects

1. Launch the Group Policy Management Console: navigate to **Start** → **Run**, type in gpmc.msc and click **OK**.
2. In the Group Policy Management Console, expand the **Forest: <your_forest_name>** node, right-click **Domains** and select **Manage Backups** from the drop-down menu.
3. In the **Manage Backups** dialog, click **Browse** and select the folder with Group Policy backup files. The folders with backup files are usually named by dates, so you can pick a folder by the required date. You will be presented with a list of Group Policy objects backed up on the selected date:

Figure 49: Group Policy Management Console



Backup location: Data\NetWrix\Management Console\Data\AD Changes\nwx.local\2009_5_26_7_0_14.gpcr

Browse...

Backed up GPOs:

Domain	Name	Time Stamp	Description	GPO ID
nwx.local	Default Domai...	5/26/2009 10:01:18 AM		{31B2F340-016...
nwx.local	Default Domai...	5/26/2009 10:01:40 AM		{6AC1786C-016...

□ Show only the latest version of each GPO

Restore | Delete | View Settings... | Close

4. Select the required object in the **Backed up GPOs** grid and click the **Restore** bottom button.

Note: By default, saving of the backup files is disabled. To enable the saving, set the GPOBackup registry key value to 1.

Copyright © 2012 NetWrix Corporation. All Rights Reserved

A APPENDIX: REGISTRY KEYS

The table below contains the description of the basic NetWrix Group Policy Change Reporter registry keys that you may need to configure while using the product. To configure a registry key, navigate to **Start → Run**, type in **regedit** and start Registry Editor.

Table 11: NetWrix Group Policy Change Reporter Registry Keys

Registry Key	Type	Description/Value	Created during setup	Preserved during upgrade
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
GPOBackup	REG_DWORD	Defines whether to backup GPOs during data collection: 0 - no 1- yes	Yes	No
GPOBackupDays	REG_DWORD	Defines the backup frequency: 0 - backup always X - once in X days Note: GPOBackup must be set to 1	Yes	No
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
ShortEmailSubjects	REG_DWORD	Defines whether to contract the email subjects (e.g. NetWrix Group Policy	No	No

Registry Key	Type	Description/Value	Created during setup	Preserved during upgrade
		Change Reporter: Summary Report – GPCR Report): 0-no 1 - yes		
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 email: 0 – no 1 – yes	Yes	No
ShowReportGeneratorServer	REG_DWORD	Defines whether to display the report generation server in the Change Summary footer: 0 – no 1 – yes	Yes	No
ShowSummaryInFooter	REG_DWORD	Defines whether to display the summary in the Change Summary footer: 0 – no 1 – yes	Yes	No
ShowSummaryInHeader	REG_DWORD	Defines whether to display the summary 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 DCs 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	No	Yes

Registry Key	Type	Description/Value	Created during setup	Preserved during upgrade
		overwrite the database connection settings (stored in the reports data source) if they differ from the SQL server settings specified when configuring the Managed Object 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

Copyright © 2012 NetWrix Corporation. All Rights Reserved

B APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support NetWrix Group Policy Change Reporter:

Table 12: Product Documentation

Document Name	Overview
NetWrix Group Policy Change Reporter Administrator’s Guide	The current document. Provides a detailed explanation of the NetWrix Group Policy Change Reporter features and step-by-step instructions on how to configure and use the product.
NetWrix Group Policy 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 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 Administrator’s Guide	Provides a detailed explanation of the NetWrix Active Directory Change Reporter features and step-by-step instructions on how to configure and use the product.
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.
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.
Troubleshooting Incorrect Reporting of the “Who Changed” Parameter	Step-by-step instructions on how to troubleshoot incorrect reporting of the ‘who changed’ parameter.
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.

Copyright © 2012 NetWrix Corporation. All Rights Reserved