NetWrix Event Log Manager

Administrator's Guide

Product Version: 4.0

July/2012

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from NetWrix Corporation of any features or functions discussed. NetWrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice.

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

Disclaimers

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

Table of Contents

1. INTRODUCTION

1.1. Overview

This guide contains an overview of the NetWrix Event Log Manager functionality, and detailed step-by-step instructions on how to configure and use the product. It is intended for system administrators and integrators.

1.2. How This Guide Is Organized

This section explains how this guide is organized and provides a brief overview of each chapter.

- Chapter 1 Introduction: the current chapter. It explains the purpose of this document, defines its audience and explains its structure.
- Chapter 2 Product Overview: contains an overview of the product functionality, lists its main features and explains its workflow. It also contains information on licensing.
- Chapter 3 NetWrix Enterprise Management Console Overview: contains a description of the NetWrix Enterprise Management Console features and provides links to the related information.
- Chapter 4 Configuring Managed Objects: explains how to create and configure a Managed Object using the Managed Object wizard and how to modify the Managed Object settings.
- Chapter 5 Configuring Reports: provides instructions on how to configure reports based on Microsoft SQL Server Reporting Services.
- Chapter 6 Configuring Subscriptions to Reports: explains how to configure automatic reports generation and delivery.
- Chapter 7 Configuring Global Settings: provides instructions on how to configure the settings that will be applied to all existing Managed Objects and all NetWrix modules enabled for these objects.
- Chapter 8 Configuring Events Summary Options: contains an overview of the files providing additional possibilities for the events summary configuration.
- Chapter 9 Importing Audit Data: explains how to import collected data from the Audit Archive to an SQL database using the NetWrix Database Importer tool.
- Chapter 10 Data Collection: explains the data collection workflow, provides instructions on how to configure the data collection schedule and view audit data.
- Chapter 11 Reports: contains a description of all available report types, provides instructions on how to view them with examples.
- Appendix: Supporting Data: contains Event Log Manager registry keys and a list of all documents published to support NetWrix Event Log Manager.

2. PRODUCT OVERVIEW

2.1. Key Features and Benefits

NetWrix Event Log Manager is a tool for event log consolidation and archiving and for real-time alerting on specified events. NetWrix Event Log Manager provides the following functionality:

- Consolidation of all event log and syslog entries from an entire network into a central location.
- Compression and archiving of collected data for convenient analysis, prevention of data loss and audit purposes.
- Storage of event log entries in a SQL database.
- Detection of critical events and sending of email alerts.
- Reports based on SQL Server Reporting Services, with filtering, grouping and sorting; predefined reports for GLBA, HIPAA, SOX, and PCI regulatory compliances.
- Historical reporting for any specified period of time.

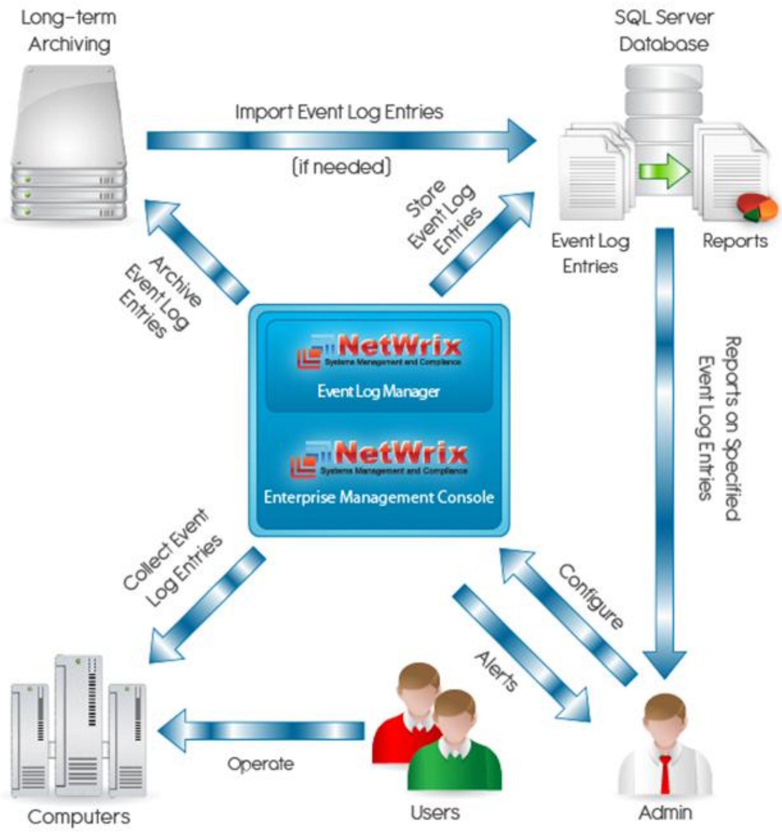
2.2. Product Workflow

A typical Event Log Manager data collection and reporting workflow is as follows:

1. The administrator configures Managed Objects, i.e. collections of computers that will be monitored.
2. The administrator sets parameters for automated data collection, and defines types of events that must be written to the Audit Archive (local file storage) and/or an SQL database. It is also possible to specify events that must trigger real-time alerts.
3. NetWrix Event Log Manager collects all new event log entries and archives them in the Audit Archive. Archived audit data can be viewed using the NetWrix Event Viewer tool.
4. If an event that triggers an alert is detected, an email notification is sent to the specified recipients.
5. If the Reports feature is enabled and configured, audit data is also written to a specified SQL database. You can generate various detailed SSRS-based reports using a set of pre-defined report templates. SSRS-based reports can be viewed either in NetWrix Enterprise Management Console, or in a web browser. Also, you can subscribe to these reports and receive them by email.
6. An events summary is emailed to the specified recipients every 24 hours by default, or on request.

The following figure illustrates the NetWrix Event Log Manager workflow:

Figure 1: NetWrix Event Log Manager Workflow


Long-term Archiving
Import Event Log Entries
(if needed)
SQL Server Database
Event Log Entries
Reports
Archive Event Log Entries
Store Event Log Entries
NetWrix Systems Management and Compliance
Event Log Manager
NetWrix Systems Management and Compliance
Enterprise Management Console
Reports on Specified Event Log Entries
Collect Event Log Entries
Configure
Alerts
Operate
Computers
Users
Admin

2.3. Licensing Information

NetWrix Event Log Manager is available in two editions: Freeware and Enterprise. The following table outlines the difference between them:

Table 1: NetWrix Event Log Manager Editions

Feature	Freeware Edition	Enterprise Edition
Long-term archiving and reporting	Only for 1 month	Any period of time
Reports based on SQL Server Reporting Services, with filtering, grouping and sorting	No	Yes
Predefined reports for GLBA, HIPAA, SOX, and PCI regulatory compliances	No	Yes
Custom reports	No	Yes. Create manually or order from NetWrix (3 reports at no charge!)
Enterprise-class scalability	No	Yes
Subscription to reports	No	Yes
A single installation handles multiple computer collections, each with its own individual settings	No	Yes
Consolidation of all event log and syslog entries from an entire network into a central location.	Only for event logs	Yes
Integrated interface for all NetWrix products, which provides centralized configuration management	No	Yes

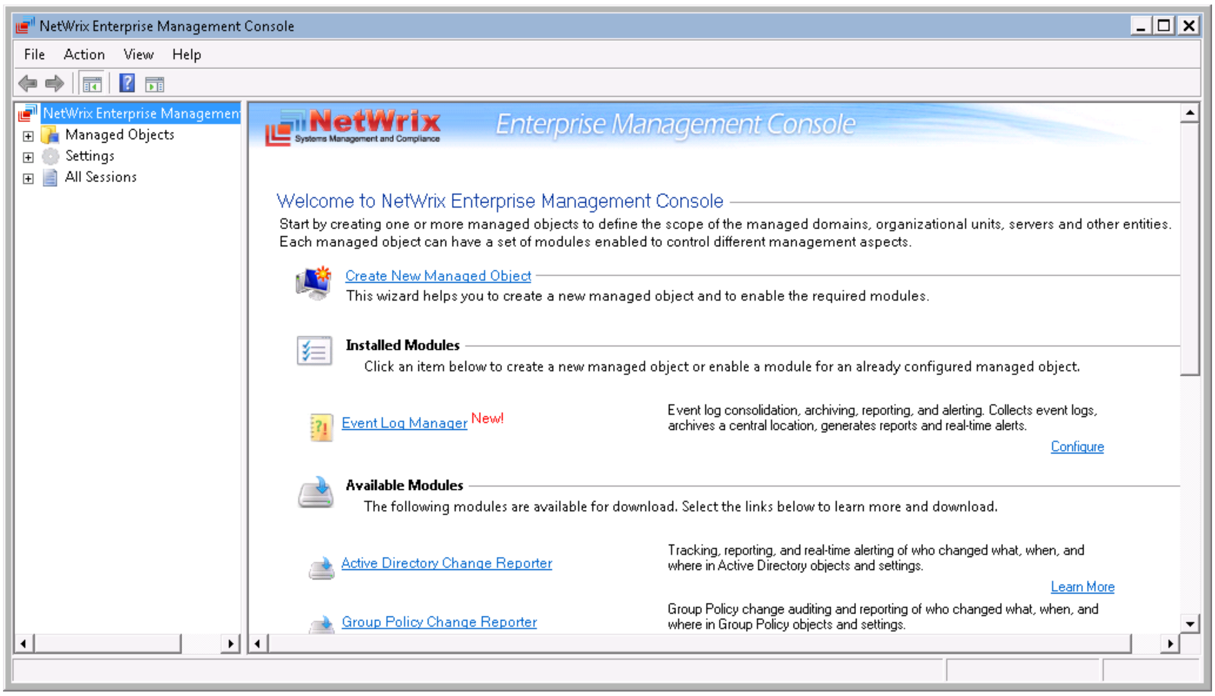
Integrated reports with lots of predefined out-of-the-box reports for all the major platforms.	No	Yes
Technical Support	Support Forum, Knowledge Base	Full range of options (phone, email, submission of support tickets, Support Forum, Knowledge Base)
Licensing	Free of charge for up to 10 servers/DCs and 100 workstations	Per monitored machine or volume license, please request a quote

3. NetWrix Enterprise Management Console Overview

NetWrix Event Log Manager Enterprise Edition is integrated into NetWrix Enterprise Management Console, which is a convenient tool that allows configuring Managed Objects, their settings and reporting options.

To start NetWrix Enterprise Management Console, navigate to **Start → All Programs → NetWrix → Event Log Manager → Event Log Manager (Enterprise Edition)**:

Figure 2: NetWrix Enterprise Management Console Main Page



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

Welcome to NetWrix Enterprise Management Console

Start by creating one or more managed objects to define the scope of the managed domains, organizational units, servers and other entities. Each managed object can have a set of modules enabled to control different management aspects.

Create New Managed Object

This wizard helps you to create a new managed object and to enable the required modules.

Installed Modules

Click an item below to create a new managed object or enable a module for an already configured managed object.

Event Log Manager New!

Event log consolidation, archiving, reporting, and alerting. Collects event logs, archives a central location, generates reports and real-time alerts.

Configure

Available Modules

The following modules are available for download. Select the links below to learn more and download.

Active Directory Change Reporter

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

Learn More

Group Policy Change Reporter

Group Policy change auditing and reporting of who changed what, when, and where in Group Policy objects and settings.

With NetWrix Enterprise Management Console you can do the following:

- Manage all NetWrix change auditing products' settings via an integrated interface
- Create and configure Managed Objects for Windows and Syslog-based platforms
- Enable and configure SSRS-based reports
- Enable and configure real-time alerts
- Enable and configure long-term archiving
- View Reports in a built-in browser
- Enable and configure subscriptions to Reports
- Configure your Managed Objects' settings in a batch

4. Configuring Managed Objects

In NetWrix Event Log Manager, a Managed Object is a computer collection that you monitor for events.

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

- Create a Managed Object
- Configure Real-Time Alerts
- Configure Audit Archiving Filters
- Modify Managed Object Settings

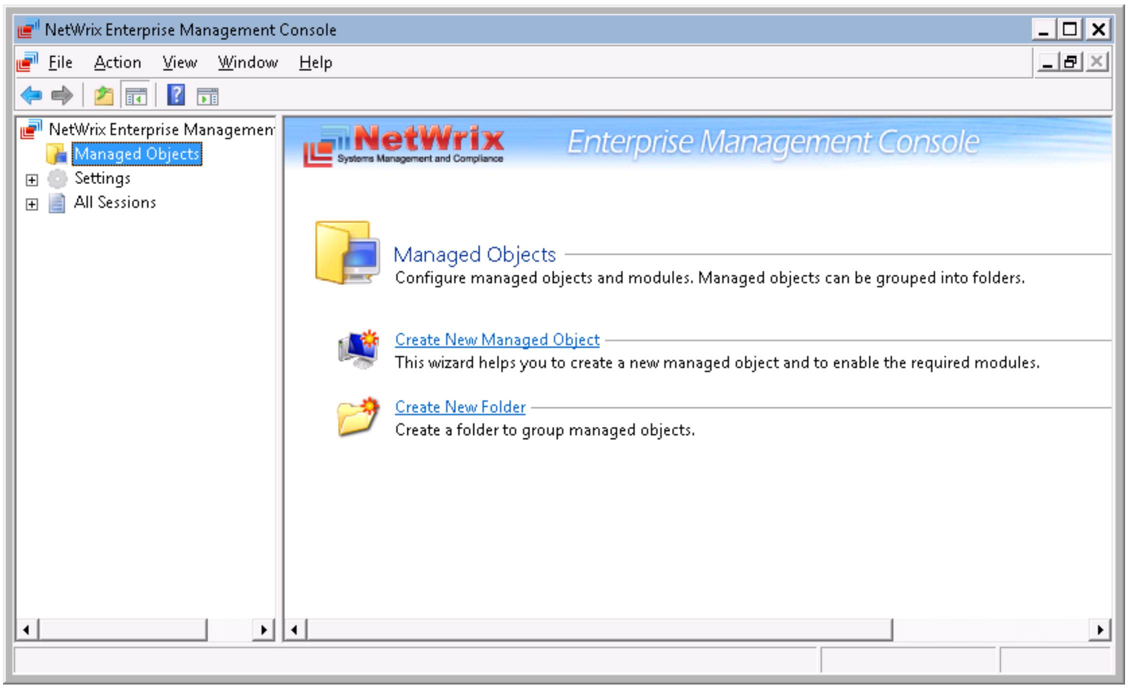
4.1. Creating a Managed Object

To create and configure a Managed Object, perform the following procedure:

Procedure 1. To create and configure a Managed Object

1. Navigate to **Start → All Programs → NetWrix → Event Log Manager → Event Log Manager (Enterprise Edition).** In NetWrix Enterprise Management Console click the **Managed Objects** node in the left pane. The Managed Objects page will be displayed:

Figure 3: Managed Objects Page


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

Managed Objects
Configure managed objects and modules. Managed objects can be grouped into folders.

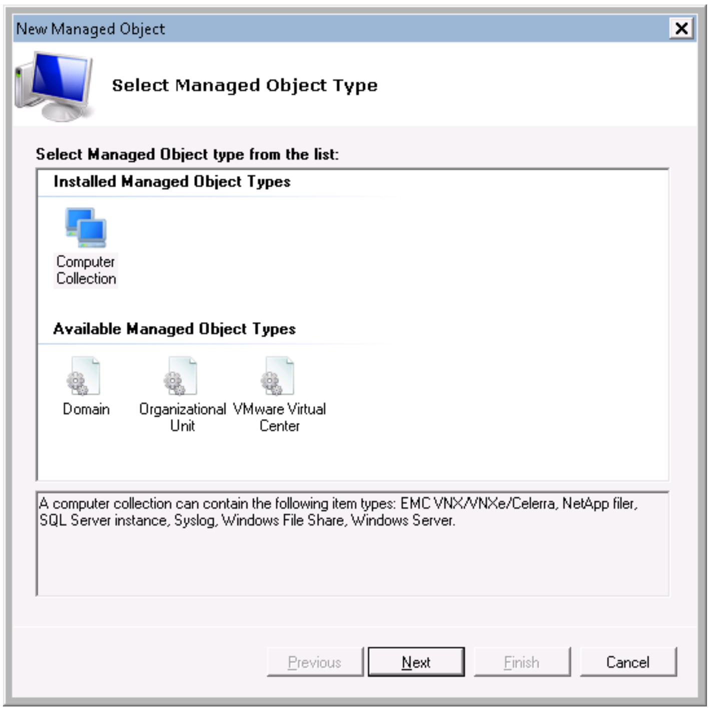
Create New Managed Object
This wizard helps you to create a new managed object and to enable the required modules.

Create New Folder
Create a folder to group managed objects.

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

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

Figure 4: New Managed Object Wizard: Selecting Managed Object Type



Select Managed Object type from the list:

A computer collection can contain the following item types: EMC VNX/VNXe/Celerra, NetApp filer, SQL Server instance, Syslog, Windows File Share, Windows Server.

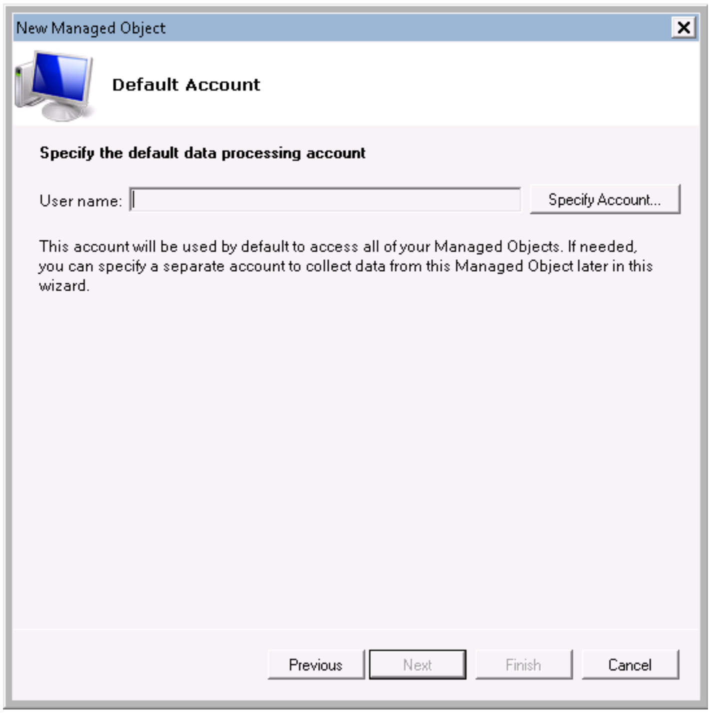
3. On the first step, select **Computer Collection** as the Managed Object type and click **Next** to continue.

   Note: If you have installed other NetWrix products previously, the list of Managed Object types may contain several options.

4. On the next step, click the **Specify Account** button:

   Note: If you have installed other NetWrix products previously and specified the default account and email settings on their configuration, steps 4-7 of this procedure will be omitted.

Figure 5: New Managed Object Wizard: Specifying the Default Account



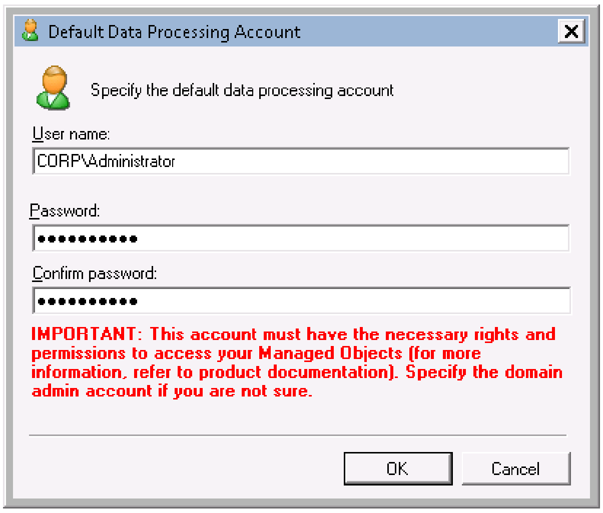
Specify the default data processing account

User name:

This account will be used by default to access all of your Managed Objects. If needed, you can specify a separate account to collect data from this Managed Object later in this wizard.

5. Enter the default data processing account (<domain name>\<account name>) that will be used by NetWrix Event Log Manager for data collection. This must be a local admin account on the computer where NetWrix Event Log Manager is installed and on the target computers. If this account is going to be used to access an SQL database, it must also belong to the target database owners (dbo) role:

Figure 6: Default Data Processing Account



Default Data Processing Account

Specify the default data processing account

User name: CORP\Administrator

Password: ••••••••••

Confirm password: ••••••••••

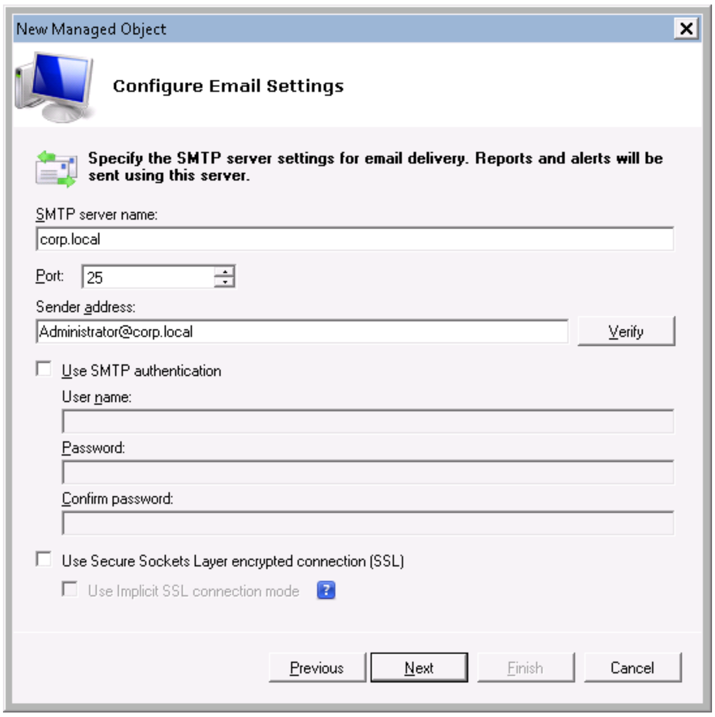
IMPORTANT: This account must have the necessary rights and permissions to access your Managed Objects (for more information, refer to product documentation). Specify the domain admin account if you are not sure.

Click **OK** to continue.

Note: If later you need to modify the default account, in NetWrix Enterprise Management Console navigate to **Settings → Schedule**. Under **Data Processing Account** click the **Change** button and specify the name and password of a new account.

6. On the next step, specify the email settings that will be used to send events summaries and reports:

Figure 7: New Managed Object Wizard: Configuring 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: corp.local

Port: 25

Sender address: Administrator@corp.local

☐ 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:

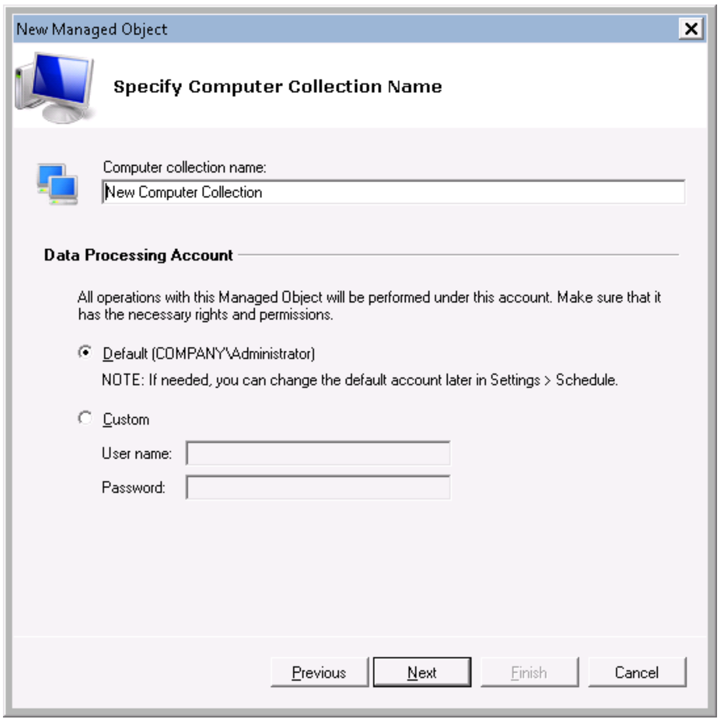
Table 2: Email Settings Parameters

Parameter	Description
SMTP server name	Enter your SMTP server name.
Port	Enter your SMTP server port number.
Sender address	Enter an email that will appear in the "From" field in reports and alerts. To check the correctness of 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 SMTP authentication.
User name	Enter a user name for SMTP authentication.
Password	Enter a password for SMTP authentication.
Confirm password	Enter a password for SMTP authentication once again.
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 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.

7. On the next step, specify your computer collection name:

Figure 8: New Managed Object Wizard: Specifying Computer Collection Name



Computer collection name: New Computer Collection

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 (COMPANY\Administrator)

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

○ Custom

User name:

Password:

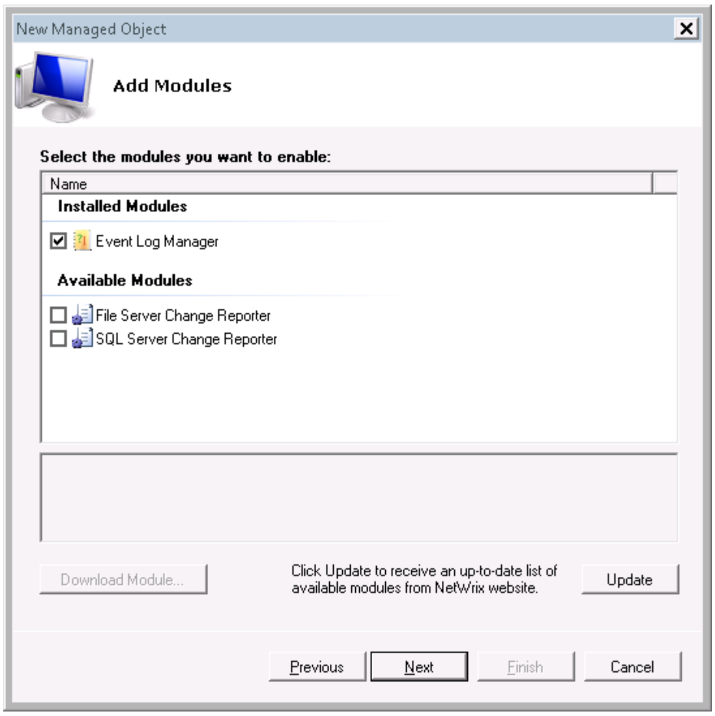
8. If you want to use a specific account to collect data from this computer collection (other than the one you specified as the default data processing account earlier in this procedure), select the **Custom** radio button and specify the credentials.

   Note: This account must be granted the same permissions and access rights as the default data processing account.

9. On the next step, make sure that NetWrix Event Log Manager is selected under **Installed Modules**:

   Note: If you have installed other NetWrix products previously, the list of installed modules may contain several options.

Figure 9: New Managed Object Wizard: Adding Modules



New Managed Object

Add Modules

Select the modules you want to enable:

Name

Installed Modules

☑ Event Log Manager

Available Modules

□ File Server Change Reporter

□ SQL Server Change Reporter

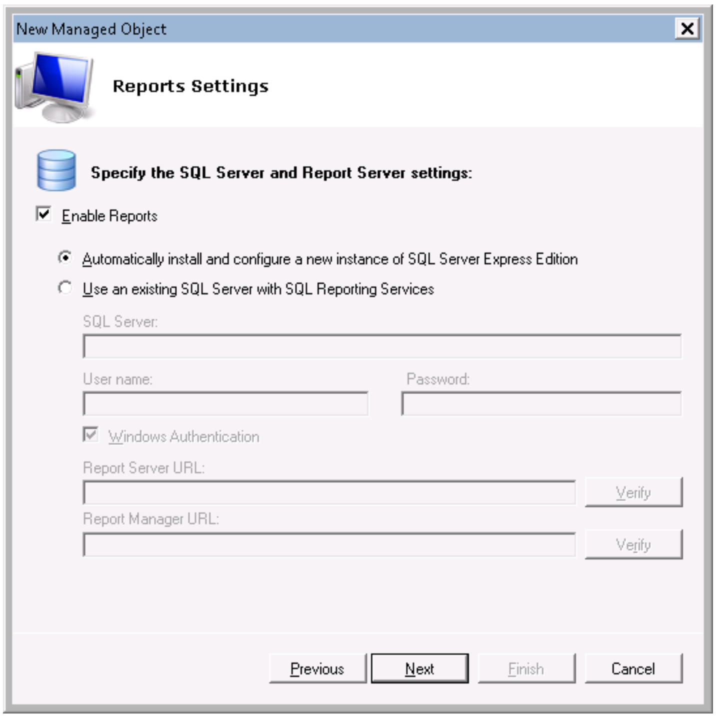
Click Update to receive an up-to-date list of available modules from NetWrix website.

On this step, under **Available Modules**, there is a list of other NetWrix products that monitor computer collection as a Managed Object type. To get more information on these products, select a module and click the **Download Module** button. You will be redirected to the product's website page.

10. To be able to use the Reports functionality, on the next step, select the **Enable Reports** option:

    Note: If you do not enable the **Reports** feature, audit data will not be written to an SQL database and you will not be able to receive SSRS-based reports.

Figure 10: New Managed Object Wizard: 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:

User name:

Password:

☑ Windows Authentication

Report Server URL:

Report Manager URL:

11. Select one of the following options:

- **Automatically install and configure a new instance of SQL Server Express Edition**: Select this option if you want the system to automatically install SQL Server 2005 Express with Advanced Services and configure the Reporting Services used by the NetWrix Event Log Manger Reports feature.

Note: It is recommended to consider 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, the events you are going to collect, etc. Note, that maximum database size in SQL Server Express editions may be insufficient.

- **Use an existing SQL Server with SQL Reporting Services**: Select this option if you want to use an already installed SQL server instance, or if you want to install and configure it manually before proceeding with NetWrix Event Log Manager configuration.

Note: For details on how to install Microsoft SQL Server 2005/2008 R2 Express and configure the Reporting Services, refer to the following NetWrix technical article: Installing Microsoft SQL Server and Configuring the Reporting Services

If the second option is selected, specify the following parameters:

Table 3: Reports Parameters

Parameter	Description
SQL Server	Specify the name of the SQL Server instance where a database of collected audit data will be created.
User name	Specify a user name for SQL Server authentication. **NOTE**: This user must belong to the target database owners (dbo) role.
Password	Specify a password for SQL Server authentication.
Windows Authentication	Select this option if you want to use the default data

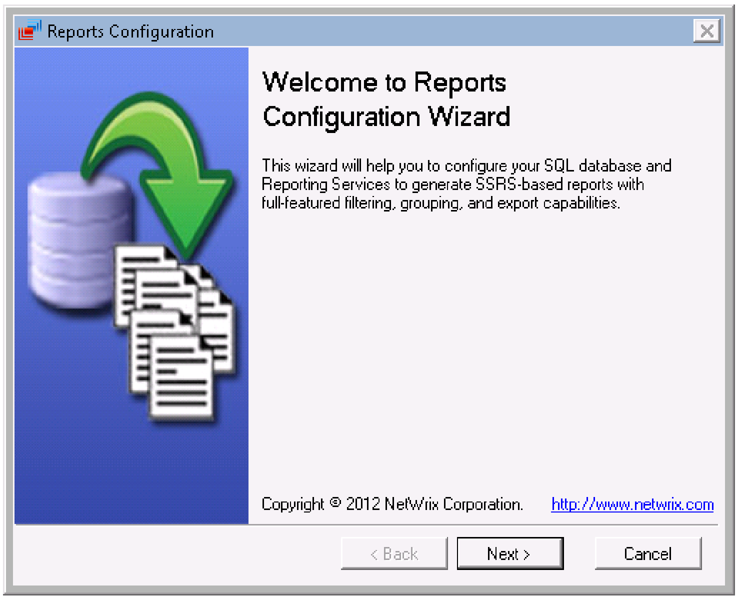
	processing account (specified earlier in this procedure) to access the SQL database.
Report Server URL	Specify the Report Server URL. **NOTE**: It is recommended to click the **Verify** button to ensure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. **NOTE**: It is 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 for this Managed Object. Also, you will only be able to select the SQL database that was previously created for other Managed Objects. If you want to write events for this Managed Object to a different SQL database, you can change the **Reports** settings after the completion of the New Managed Object wizard. For infiormation on how to change these settings, refer to Procedure 6 To specify SQL Server settings.

12. Click **Next** to continue.

    If you have selected to automatically install and configure SQL Server 2005 Express, the Reports Configuration wizard will start:

Figure 11: Reports Configuration Wizard



Reports Configuration

Welcome to Reports Configuration Wizard

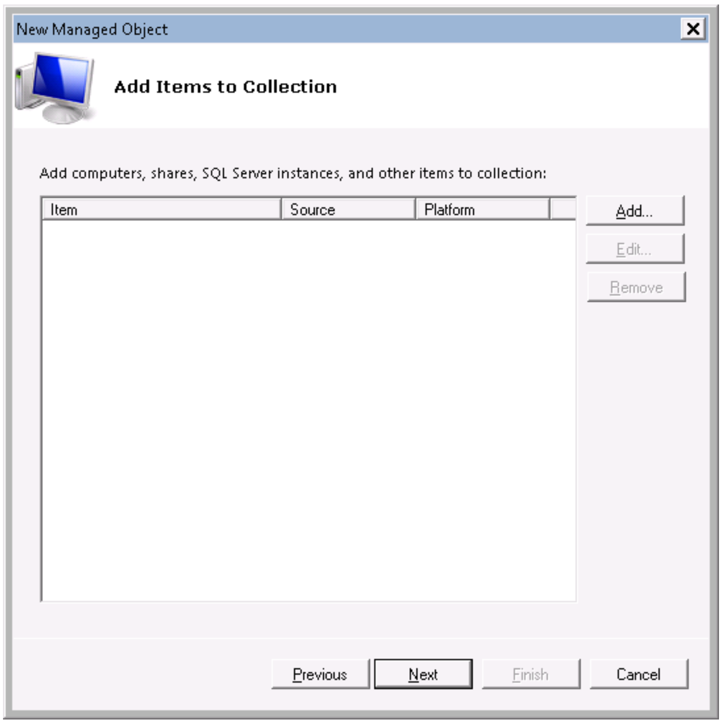
This wizard will help you to configure your SQL database and Reporting Services to generate SSRS-based reports with full-featured filtering, grouping, and export capabilities.

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

Follow the instructions of the wizard to install and configure SQL Server 2005 Express with Advanced Services.

13. On the next step, add items to your computer collection. To do this, click the **Add** button:

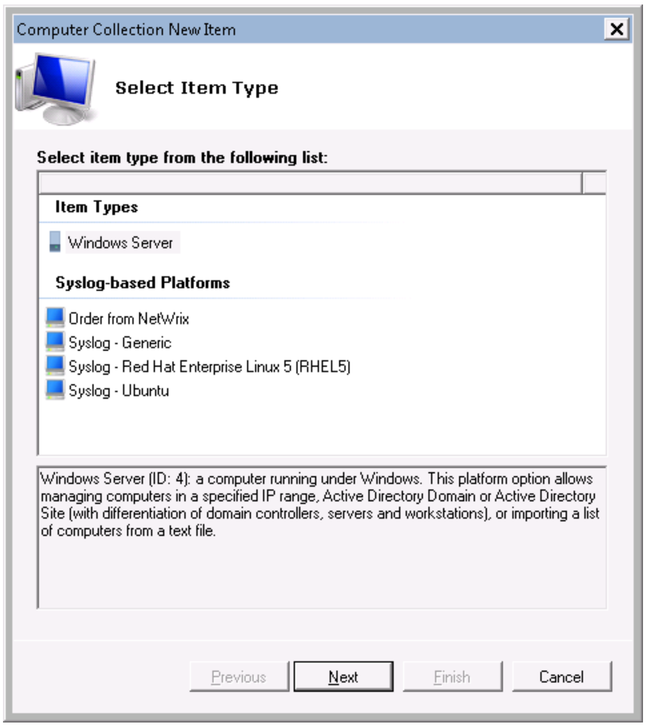
Figure 12: New Managed Object Wizard: Add Items to Collection



Add computers, shares, SQL Server instances, and other items to collection:

14. In the Computer Collection New Item wizard, select one of the predefined platform types: Windows Server or Syslog-based Platform. Also, you can order a custom syslog-based platform from NetWrix by selecting the **Order from NetWrix** option and clicking the link below:

Figure 13: New Managed Object Wizard: Select Item Type



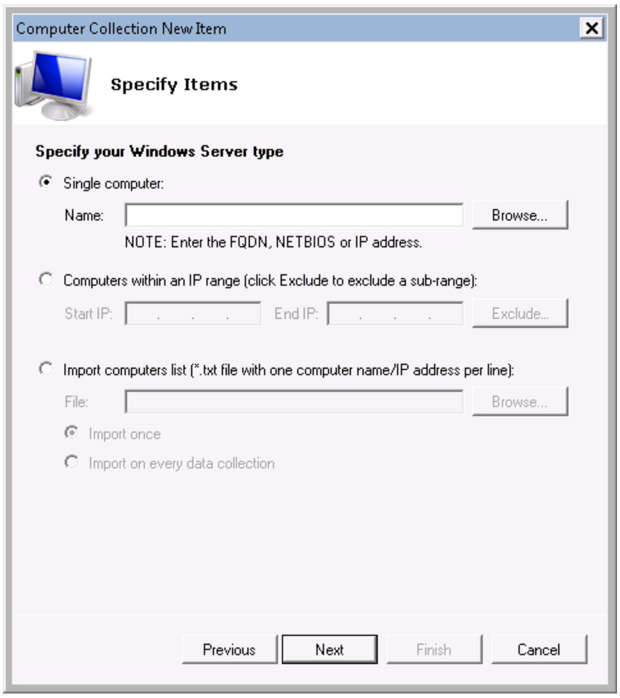
Select item type from the following list:

Windows Server (ID: 4): a computer running under Windows. This platform option allows managing computers in a specified IP range, Active Directory Domain or Active Directory Site (with differentiation of domain controllers, servers and workstations), or importing a list of computers from a text file.

Note: If you have configured custom syslog platforms previously, they will appear in the **Syslog-based Platforms** list.

15. Click **Next.**

Figure 14: Computer Collection New Item Wizard



Computer Collection New Item

Specify Items

Specify your Windows Server type

● Single computer:

Name:

NOTE: Enter the FQDN, NETBIOS or IP address.

○ Computers within an IP range (click Exclude to exclude a sub-range):

Start IP: End IP:

○ Import computers list (*.txt file with one computer name/IP address per line):

File:

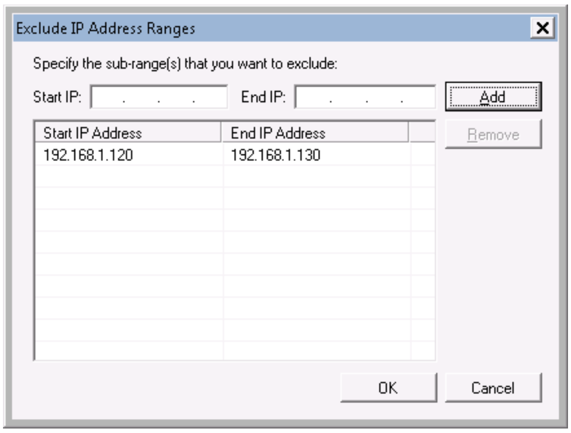
● Import once

○ Import on every data collection

The following selection options are provided:

- Single computer: allows specifying a single computer by entering its FQDN, NETBIOS name or IP address. You can click the **Browse** button to select from network computers.
- Computers within an IP range: allows specifying an IP range for computers you want to monitor. Also, you can exclude sub-ranges of IP addresses from monitoring by clicking the **Exclude** button. Enter the IP range you want to exclude, and click **Add**. Then click **OK**:

Figure 15: Exclude IP Address Ranges



Exclude IP Address Ranges

Specify the sub-range(s) that you want to exclude:

Start IP: End IP:

Start IP Address	End IP Address
192.168.1.120	192.168.1.130

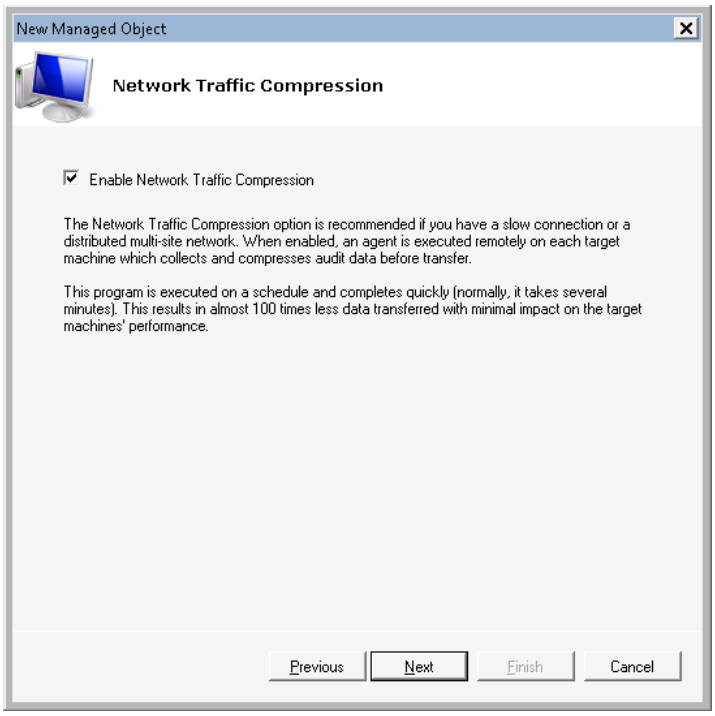
- Import computers list: allows importing computers' names from a file. This file must be in a plain text format; each line must contain the FQDN/NETBIOS/IP address of one computer. If you select to import a list of computers from a file, select one of the following options:
    - **Import once**: The list of computers will be imported once, and if later you edit this file, this will not affect your monitored computer collection.

- **Import on every data collection**: The file will be uploaded every time a scheduled data collection task is run, so you can add/remove computers from your monitored computer collection by editing this file.

16. Click **Next** to continue. Review your new item's settings and click **Finish**. It will be added to the computer collection. You can add more items if needed.

17. On the next step, you can select the **Enable Network Traffic Compression** option:

Figure 16: New Managed Object Wizard: Network Traffic Compression



☑ Enable Network Traffic Compression

The Network Traffic Compression option is recommended if you have a slow connection or a distributed multi-site network. When enabled, an agent is executed remotely on each target machine which collects and compresses audit data before transfer.

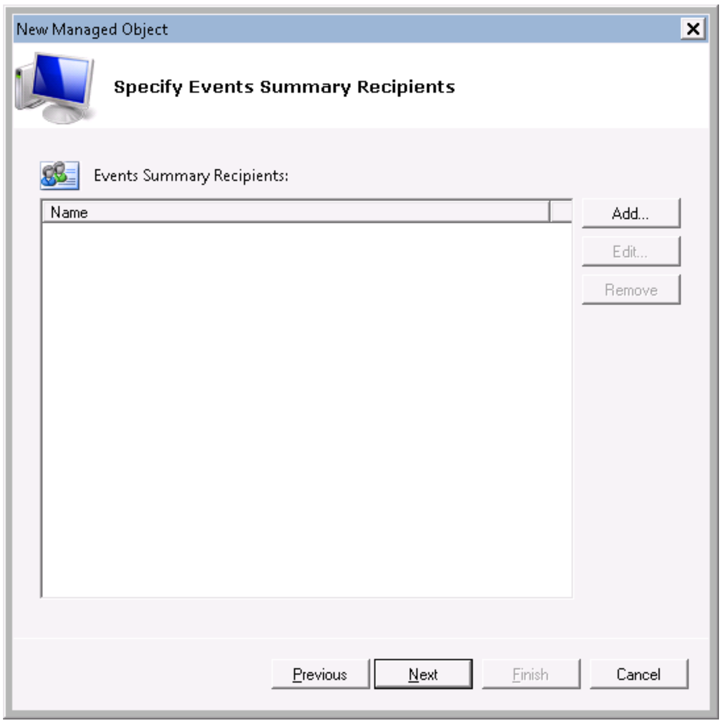
This program is executed on a schedule and completes quickly (normally, it takes several minutes). This results in almost 100 times less data transferred with minimal impact on the target machines' performance.

If this feature is enabled, an agent will be installed automatically that runs on the managed computers, collects and pre-filters data, and sends it to NetWrix Event Log Manager in a compressed format. It significantly improves data transfer and minimizes impact on target computer's performance.

Note: It is highly recommended to enable this feature for correct processing of events.

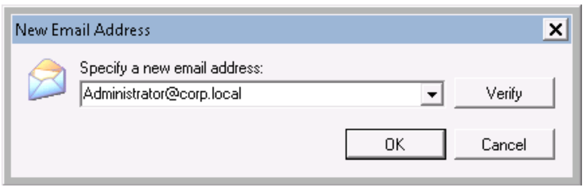
18. Click **Next** to continue. On the next step, you must specify the events summary recipient(s):

Figure 17: New Managed Object Wizard: Specifying Events Summary Recipients



Click the **Add** button and specify the email address(es) where the events summary must be delivered:

Figure 18: New Email Address



Specify a new email address: Administrator@corp.local

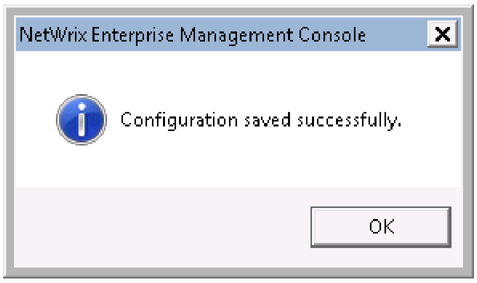
It is recommended to click the **Verify** button. The system will send a test message to the specified email address and will inform you if any problems are detected.

19. Click **Next** to continue. On the following step, you can to configure real-time alerts. For detailed instructions on how to do this, refer to Section 4.2 Configuring Real-Time Alerts.

20. On the next step, you can configure Audit Archiving Filters. For detailed instructions on how to do this, refer to Section 4.3 Configuring Audit Archiving Filters.

21. On the last step, review your Managed Object settings and click **Finish** to complete the wizard. The following confirmation message will be displayed:

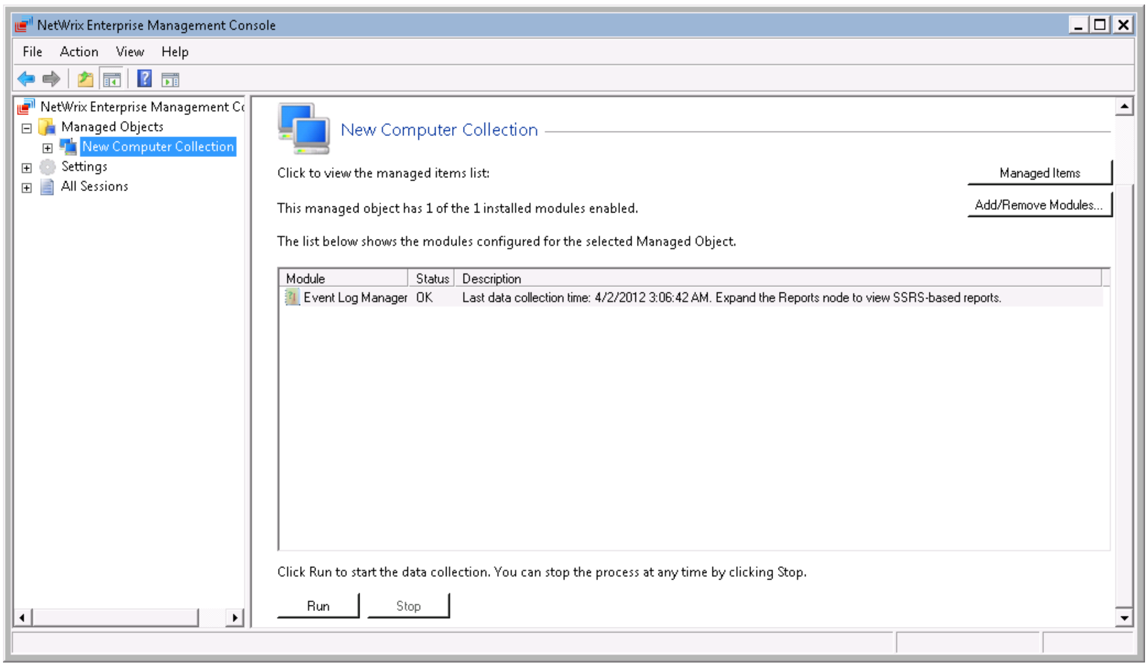
Figure 19: New Managed Object Creation Confirmation



Configuration saved successfully.

The newly created Managed Object will appear under the **Managed Objects** node, and its details will be displayed in the right pane:

Figure 20: New Managed Object Details



Click to view the managed items list:

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

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

Module	Status	Description
Event Log Manager	OK	Last data collection time: 4/2/2012 3:06:42 AM. Expand the Reports node to view SSRS-based reports.

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

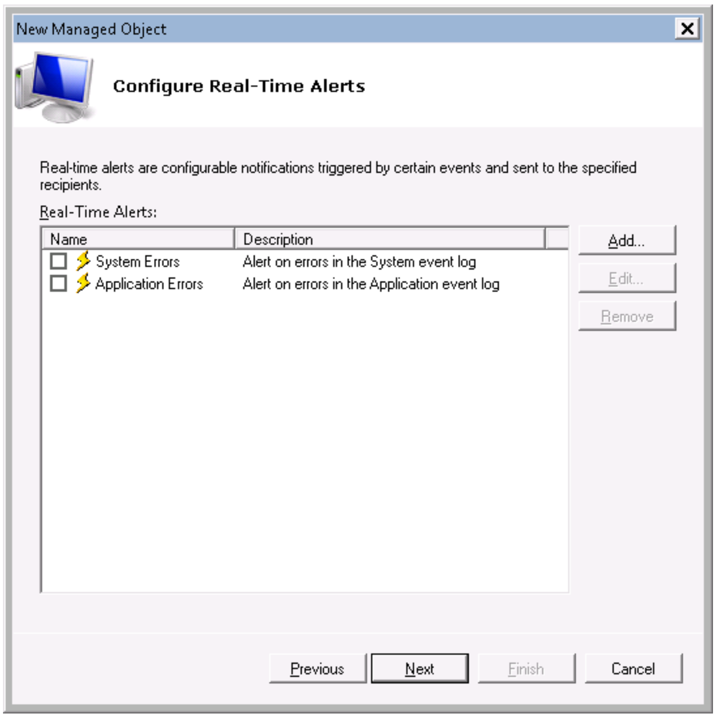
4.2. Configuring Real-Time Alerts

Real-time alerts are configured using the New Alert wizard. This wizard can be launched from the following locations:

- New Managed Object wizard

  When creating a Managed Object, the following dialog is displayed:

Figure 21: New Managed Object Wizard: Configuring Real-Time Alerts



Real-time alerts are configurable notifications triggered by certain events and sent to the specified recipients.

Name	Description
□ System Errors	Alert on errors in the System event log
□ Application Errors	Alert on errors in the Application event log

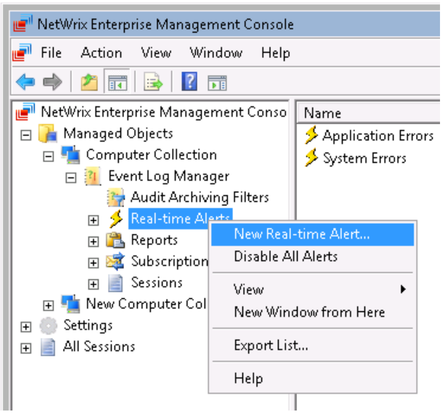
There are two predefined real-time alerts. You can enable them for this Managed Object by selecting the corresponding check-box, edit or remove these alerts.

To start the **New Alert** wizard, click the **Add** button.

- NetWrix Enterprise Management Console

  To start the **New Alert** wizard, right-click the **Real-time Alerts** node and select the **New Real-time Alert** option from the pop-up menu:

Figure 22: Launching the New Alert Wizard in NetWrix Enterprise Management Console

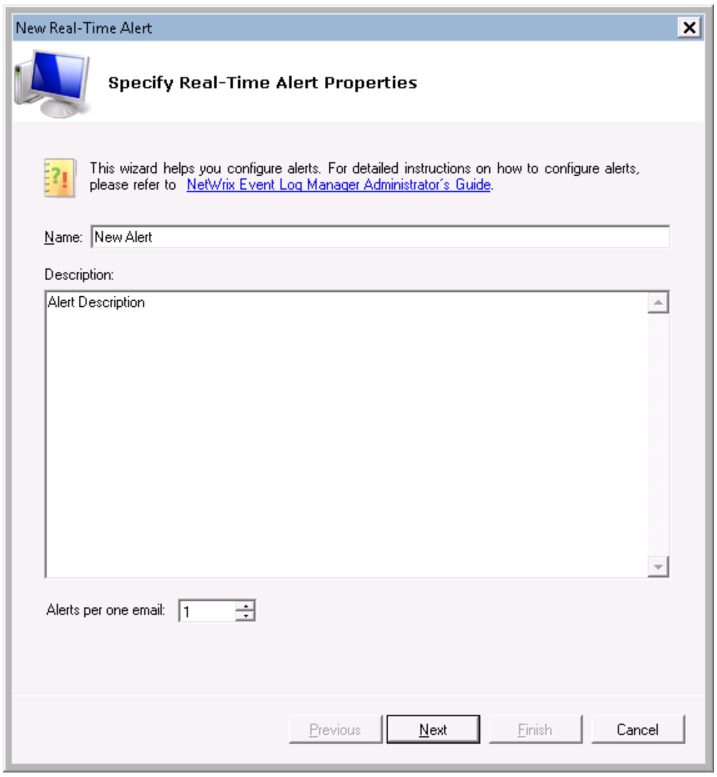


To configure a real-time alert, perform the following procedure:

Procedure 2. To configure a real-time alert

1. Launch the New Alert wizard:

Figure 23: New Alert Wizard: Specifying Real-Time Alert Properties



New Real-Time Alert

Specify Real-Time Alert Properties

This wizard helps you configure alerts. For detailed instructions on how to configure alerts, please refer to NetWrix Event Log Manager Administrator's Guide.

Name: New Alert

Description:

Alert Description

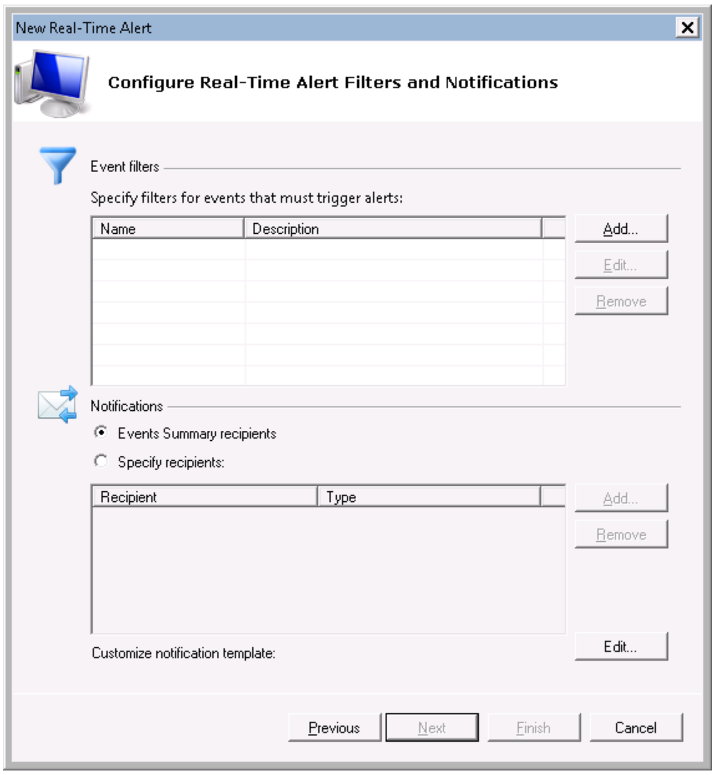
Alerts per one email: 1

2. In this dialog, specify the alert’s name and description and set the number of alerts per one email. Grouped alerts for different computers will be delivered in separate

email messages. This value is set to 1 by default, which means that each alert will be delivered as a separate email message.

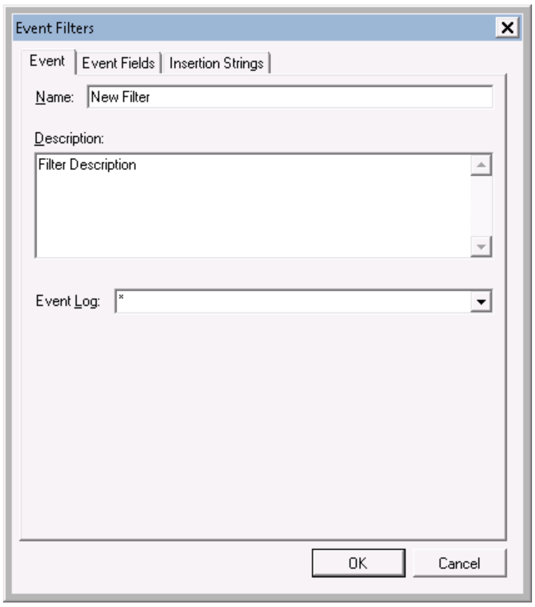
3. Click **Next**. The following dialog will be displayed:

Figure 24: New Alert Wizard: Specifying Real-time Alert Filters and Notifications


New Real-Time Alert
Configure Real-Time Alert Filters and Notifications
Event filters
Specify filters for events that must trigger alerts:
Name
Description
Add...
Edit...
Remove
Notifications
● Events Summary recipients
○ Specify recipients:
Recipient
Type
Add...
Remove
Customize notification template:
Edit...
Previous
Next
Finish
Cancel

4. In the **Configure Real-Time Alert Filters and Notifications** dialog, you must specify at least one event filter that will trigger the alert. To add a new filter, click the **Add** button under **Event filters**. The following dialog will be displayed:

Figure 25: Event Filters



Name: New Filter

Description: Filter Description

Event Log: *

Specify the following parameters:

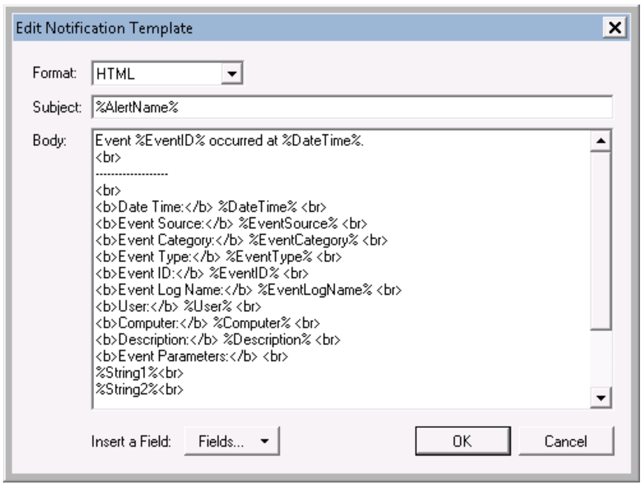
Table 4: Event Filter Parameters

Parameter	Description
Event tab	
Name	Enter the event filter name.
Description	Enter the event filter description (optional).
Event Log	Select an event log from the drop-down list. You will only be alerted on events from this event log. You can also specify a different event log. The correct event log’s name you can find in the **Full Name** field of the **Log Properties** dialog. To find out a log’s name, navigate to **Start → Control Panel → Administrative Tools → Event Viewer → Applications and Services Logs,** expand the **Microsoft** node and select **Windows**. Then expand the Windows node and the required **<Log_Name>** node, right-click the file under it and select **Properties** from the pop-up menu. On the **Log Properties** dialog **General** tab, find the event log’s name in the **Full Name** field. NetWrix Event Log Manager does not collect the Analytic and Debug logs, so you cannot configure alerts for these logs. **NOTE**: You can use a wildcard (*). In this case you will be alerted on events from all Windows logs except for the ones mentioned above. Syslog events will be ignored.
Event Fields tab	
Event ID	Enter the identifier of a specific event that you want to be alerted on. You can add several IDs separated by comma.
Event Level	Select the event types that you want to be alerted on. If the Event Level check box is cleared, you will be alerted on all event types of the specified log.
Computer	Specify a computer. You will only be alerted on events from this computer. **NOTE**: If you need to specify several computers, you can define a mask for this parameter. Below is an example of a mask: • * - any machine • computer -a machine named ‘computer’ • *computer* - machines with names like ‘xXxcomputerxXx’ or ‘newcomputer’ • computer? – machines with names like ‘computer1’ or ‘computerV’ • co?puter - machines with names like ‘computer’ or ‘coXputer’ • ????? – any machine with a 5-character name • ???* - any machine with a 3-character name or longer
User	Enter a user’s name. You will be alerted only on the events generated under this account. **NOTE**: If you need to specify several users, you can define a mask for this parameter in the same way as for the **Computer** entry field.
Source	Specify this parameter if you want to be alerted on the events from a specific source. **NOTE**: If you need to specify several sources, you can define a mask for this parameter in the same way as for the **Computer** entry field.

Category	Specify this parameter if you want to be alerted on a specific event category.
Insertion Strings tab	
Consider the following event Insertion Strings	Specify this parameter if you want to receive alerts on events containing a specific string in the EventData. You can use a wildcard (*).

Customize the notification template if needed. To do this, in the **Configure Real-Time Alert Filters and Notifications** dialog, click the **Edit** button next to **Customize notifications template**. The following dialog will open:

Figure 26: Edit Notification Template



Format: HTML

Subject: %AlertName%

Body:

```
Event %EventID% occurred at %DateTime%.
<br>
-------------------
<br>
<b>Date Time:</b> %DateTime% <br>
<b>Event Source:</b> %EventSource% <br>
<b>Event Category:</b> %EventCategory% <br>
<b>Event Type:</b> %EventType% <br>
<b>Event ID:</b> %EventID% <br>
<b>Event Log Name:</b> %EventLogName% <br>
<b>User:</b> %User% <br>
<b>Computer:</b> %Computer% <br>
<b>Description:</b> %Description% <br>
<b>Event Parameters:</b> <br>
%String1%<br>
%String2%<br>
```

5. In the **Configure Real-Time Alert Filters and Notifications** dialog, specify the addresses for alerts delivery. If you want notifications to be delivered to the email address specified in the previous step, select the **Events Summary recipients** radio button under **Notifications**. Alternatively, you can configure alerts delivery to other email addresses.
6. Edit the template by deleting or inserting information fields.
7. Click **Next** to continue. Review your real-time alert settings and click **Finish**. A new real-time alert will be added.

4.3. Configuring Audit Archiving Filters

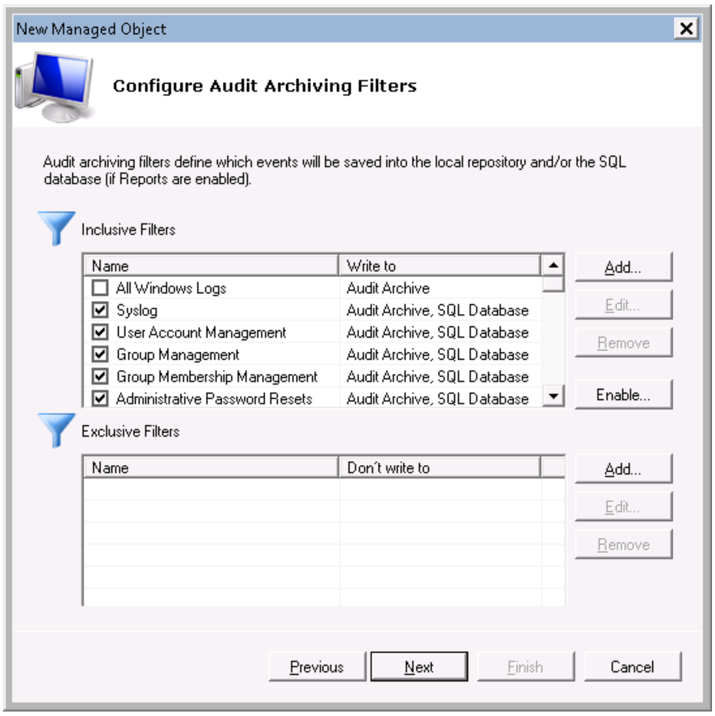
Audit archiving filters define which events will be saved into the Audit Archive and/or a SQL database (if the **Reports** feature is enabled).

> **Note:** Real-time alert filters and audit archiving filters are not related, and the latter do not affect the alerts functionality.

Audit archiving filters can be configured using:

- The New Managed Object wizard. When creating a Managed Object, the following dialog is displayed:

Figure 27: New Managed Object Wizard: Audit Archiving Filters



Audit archiving filters define which events will be saved into the local repository and/or the SQL database (if Reports are enabled).

Inclusive Filters

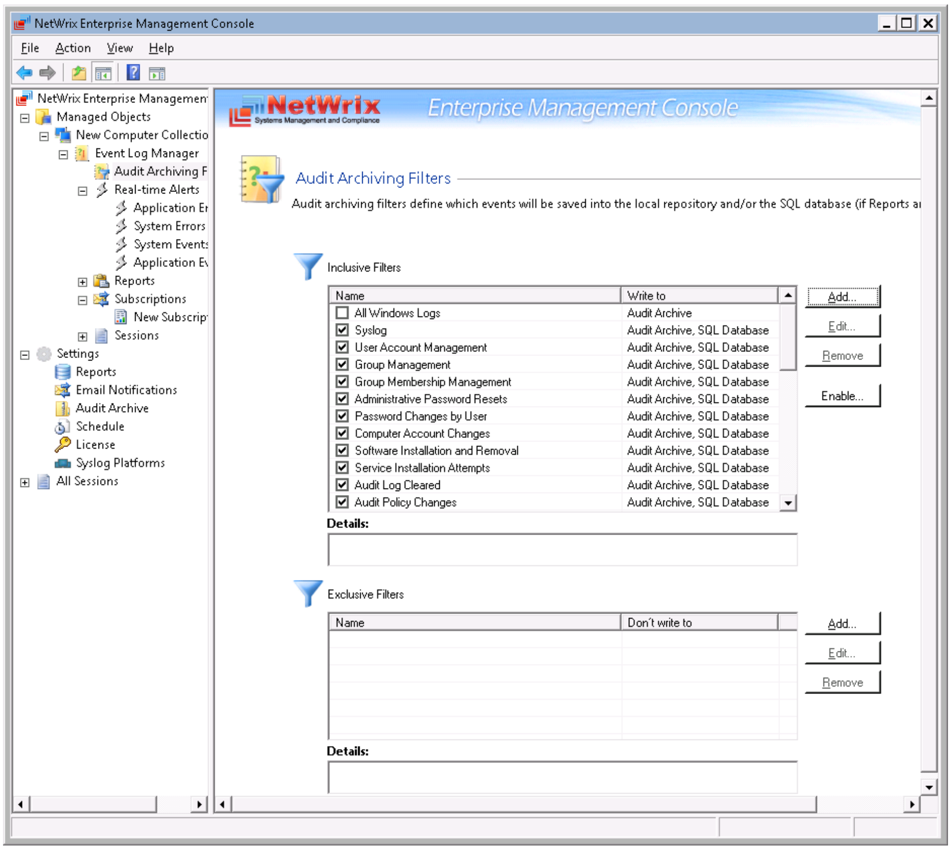
Name	Write to
□ All Windows Logs	Audit Archive
☑ Syslog	Audit Archive, SQL Database
☑ User Account Management	Audit Archive, SQL Database
☑ Group Management	Audit Archive, SQL Database
☑ Group Membership Management	Audit Archive, SQL Database
☑ Administrative Password Resets	Audit Archive, SQL Database

Exclusive Filters

Name	Don't write to

- Enterprise Management Console. Click the **Audit Archiving Filters** node to display the settings in the right pane:

Figure 28: Audit Archiving Filters Settings



Audit Archiving Filters

Audit archiving filters define which events will be saved into the local repository and/or the SQL database (if Reports a

Inclusive Filters

Name	Write to
□ All Windows Logs	Audit Archive
☑ Syslog	Audit Archive, SQL Database
☑ User Account Management	Audit Archive, SQL Database
☑ Group Management	Audit Archive, SQL Database
☑ Group Membership Management	Audit Archive, SQL Database
☑ Administrative Password Resets	Audit Archive, SQL Database
☑ Password Changes by User	Audit Archive, SQL Database
☑ Computer Account Changes	Audit Archive, SQL Database
☑ Software Installation and Removal	Audit Archive, SQL Database
☑ Service Installation Attempts	Audit Archive, SQL Database
☑ Audit Log Cleared	Audit Archive, SQL Database
☑ Audit Policy Changes	Audit Archive, SQL Database

Details:

Exclusive Filters

Name	Don't write to

Details:

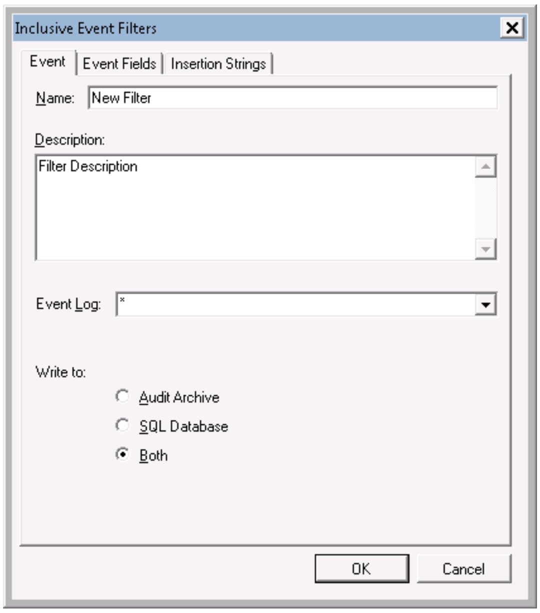
To configure audit archiving filters, you can perform the following operations:

Suggestions or comments about this document? www.netwrix.com/feedback

- To collect events required to generate a specific report, you must select a filter whose name coincides with this report's name. You can click the **Enable** button and select **Filters for Reports**. All filters required to store events for all available reports will be selected automatically.
- To select filters required to collect events for regulatory compliances (GLBA, HIPAA, PCI, SOX), click the **Enable** button, click **Select compliance** and choose the required regulation.
- To create or change an audit archiving filter, perform the following steps either in the **New Managed Object** wizard or in NetWrix Enterprise Management Console:

a. Click **Add** or **Edit** to create a new or modify an existing filter respectively. The following dialog will open:

Figure 29: Inclusive Event Filters



Name: New Filter

Description: Filter Description

Event Log: *

Write to:

○ Audit Archive

○ SQL Database

● Both

b. Specify the following parameters and click **OK** to save the changes:

Table 5: Event Filter Parameters

Parameter	Description
Event tab	
Name	Enter the event filter name.
Description	Enter the event filter description (optional).
Event Log	Select an event log from the drop-down list. You will only be alerted on events from this event log. You can also specify a different event log. The correct event log's name you can find in the **Full Name** field of the **Log Properties** dialog. To find out a log's name, navigate to **Start → Control Panel → Administrative Tools → Event Viewer → Applications and Services Logs,** expand the **Microsoft** node and select **Windows**. Then expand the Windows node and the required **<Log_Name>** node, right-click the file under it and select **Properties** from the pop-up menu. On the **Log Properties** dialog **General** tab, find the event log's name in the **Full Name** field. NetWrix Event Log Manager does not collect the Analytic and Debug logs, so you cannot configure alerts for these

	logs. By selecting the Syslog option, the events from Syslog-based platforms only will be processed. Events from custom Windows logs with the same name will not be collected. **NOTE**: You can use a wildcard (*). In this case: • For inclusive filters: all Windows logs except for the ones mentioned above will be saved. Syslog events will be ignored. • For exclusive filters: all Windows logs events will be excluded. Syslog events will be stored.
Write to	Select the location to write events to. **NOTE:** It is recommended to write the same events to the Audit Archive and to a SQL database, because if your database is corrupted, you will be able to import the necessary data from the Audit Archive using the NetWrix Database Importer tool.
Event Fields tab	
Event ID	Enter the identifier of a specific event that you want to save. You can add several IDs separated by comma.
Event Level	Select the event types that you want to save. If the **Event Level** check box is cleared, all event types will be saved. **NOTE**: If your monitored computers run Windows Vista and above and you want to select the inclusive Success Audit/Failure Audit filters, note that on these platforms these events belong to the “Information” level, so they will not be collected if you select the Information check box in the Exclusive Filters.
Computer	Specify a computer. Only events from this computer will be saved. **NOTE**: If you need to specify several computers, you can define a mask for this parameter. Below is an example of a mask: • * - any machine • computer -a machine named ‘computer’ • *computer* - machines with names like ‘xXxcomputerxXx’ or ‘newcomputer’ • computer? - machines with names like ‘computer1’ or ‘computerV’ • co?puter - machines with names like ‘computer’ or ‘coXputer’ • ????? - any machine with a 5-character name • ???* - any machine with a 3-character name or longer
User	Enter a user’s name. Only events created by this user will be saved. **NOTE**: If you need to specify several users, you can define a mask for this parameter in the same way as for the **Computer** entry field.
Source	Specify this parameter if you want to save events from a specific source. **NOTE**: If you need to specify several sources, you can define a mask for this parameter in the same way as for the **Computer** entry field.
Category	Specify this parameter if you want to save a specific events category.
Insertion Strings tab	

Consider the following event Insertion Strings	Specify this parameter if you want to store events containing a specific string in the EventData. You can use a wildcard (*).

4.4. Modifying Managed Object Settings

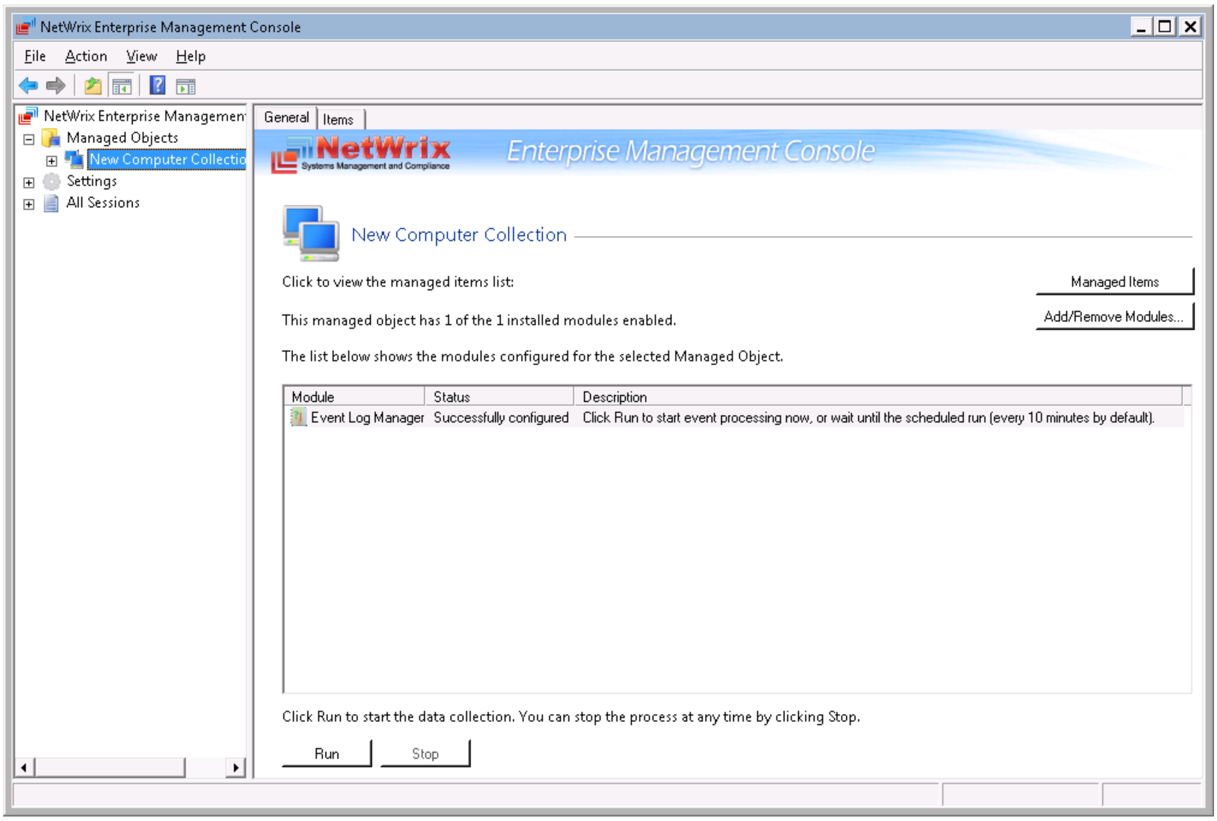
If later you need to modify an existing Managed Object's settings, perform one of the following procedures:

- Procedure 3 To modify general Managed Object settings: to enable or disable NetWrix modules for the selected Managed Object.
- Procedure 4 To edit computer collection items list: to add, remove or edit items in your computer collection.
- Procedure 5 To modify the Event Log Manager settings: to modify the product settings.

Procedure 3. To modify general Managed Object settings

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** node and select your Managed Object. The following page will be displayed with the list of NetWrix modules enabled for this Managed Object:

Figure 30: Computer Collection Page



Click to view the managed items list:

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

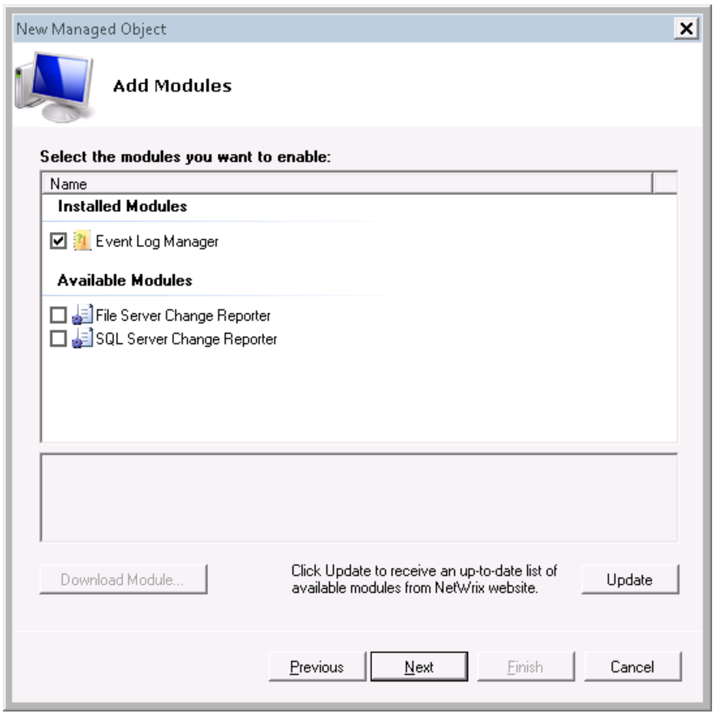
The list below shows the modules configured for the selected Managed Object.

Module	Status	Description
Event Log Manager	Successfully configured	Click Run to start event processing now, or wait until the scheduled run (every 10 minutes by default).

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

2. To enable or remove NetWrix modules for this Managed Object, click the **Add/Remove Modules** button. A window containing a list of installed and available modules will be displayed:

Figure 31: Add/Remove Modules



New Managed Object

Add Modules

Select the modules you want to enable:

Name

Installed Modules

☑ Event Log Manager

Available Modules

□ File Server Change Reporter
□ SQL Server Change Reporter

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

Note: If you have installed other NetWrix products previously, the list of installed modules may contain several options.

Under **Available Modules**, there is a list of other NetWrix products that monitor computer collection as a Managed Object type. To get more information on these products, select a module and click the **Download Module** button. You will be redirected to the product's website page.

3. To enable an installed module to monitor your Managed Object, select the corresponding check box. To remove an installed module, deselect the corresponding check box.

Note: By removing a module, you simply disable it for this Managed Object. The corresponding NetWrix product will not be uninstalled. If only one module is enabled for your Managed Object, you will not be able to remove it.

4. Click **Next**.

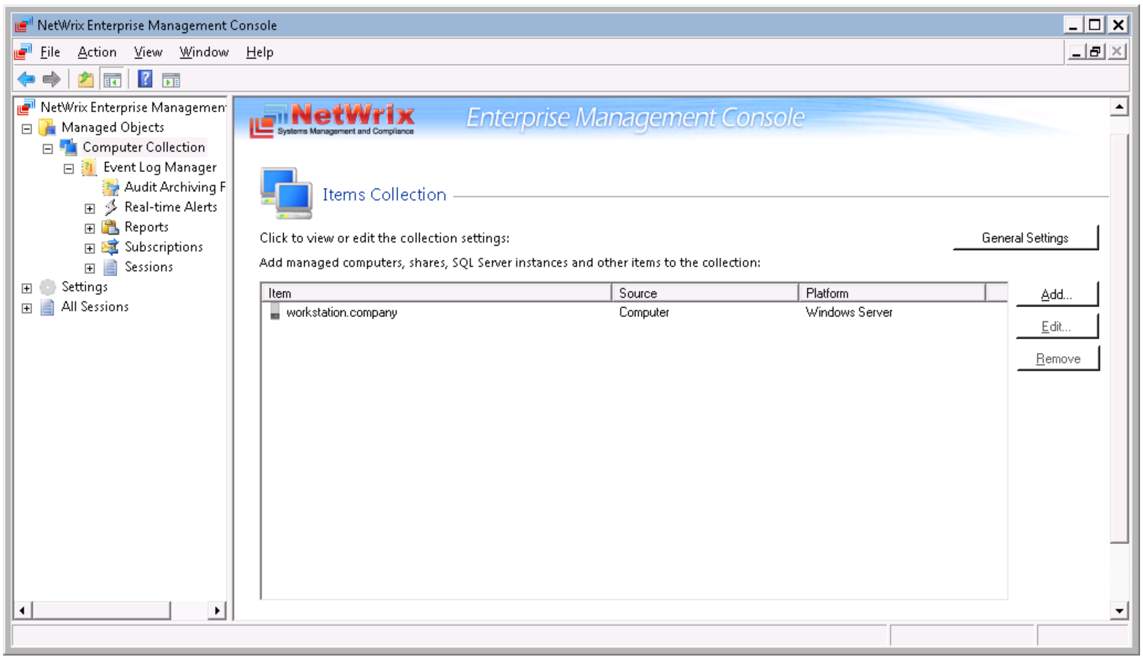
5. On the next step, you can add an item to your computer collection. For detailed instructions on how to add an item, refer to Step 13 of Procedure 1 To create and configure a Managed Object.

6. On the last step, review your Managed Object settings and click **Finish**.

Procedure 4. To edit computer collection items list

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** node, select your Managed Object, and open the **Items** tab in the right pane, or click the **Managed Items** button. The following page will be displayed with the list of items that belong to your computer collection:

Figure 32: Items Collection Page



Items Collection

Click to view or edit the collection settings:

Add managed computers, shares, SQL Server instances and other items to the collection:

Item	Source	Platform
workstation.company	Computer	Windows Server

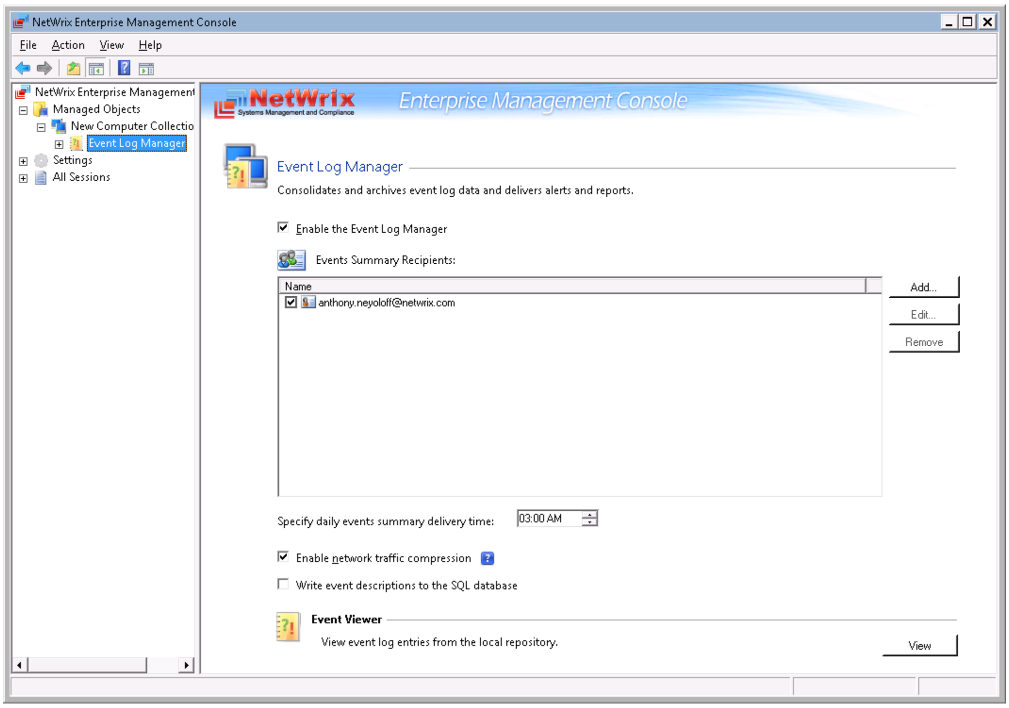
2. Use the following buttons to edit the list:

- **Add**: Click this button to add a new computer to the collection.
- **Import:** Click this button to import computer names from a file (a *.txt file with one entry per line).
- **Remove:** Use this button to delete a computer from the list.

Procedure 5. To modify the Event Log Manager settings

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<your_managed_object>** node, and select **Event Log Manager**. The following page will be displayed:

Figure 33: Managed Object Settings


NetWrix Enterprise Management Console
File
Action
View
Help
NetWrix Enterprise Management
Managed Objects
New Computer Collectio
Event Log Manager
Settings
All Sessions
NetWrix
Systems Management and Compliance
Enterprise Management Console
Add...
Edit...
Remove
View

Event Log Manager

Consolidates and archives event log data and delivers alerts and reports.

☑ Enable the Event Log Manager

Events Summary Recipients:

Name
☑ anthony.neyoloff@netwrix.com

Specify daily events summary delivery time: 03:00 AM

☑ Enable network traffic compression

□ Write event descriptions to the SQL database

Event Viewer

View event log entries from the local repository.

2. Perform one of the following operations if necessary:

- To disable (or enable, if disabled) the Event Log Manager module for this Managed Object, deselect/select the corresponding check box.

- To add an email address to the Events Summary Recipients list, click the **Add** button. Specify the email address you want to add and click **OK**. To check the correctness of 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.

- To modify an email address in the Events Summary Recipients list, select it from the list and click the **Edit** button. Edit the address and click **OK**.

- To remove an email address from the Events Summary Recipients list, select it from the list and click the **Remove** button. The selected address will be removed from the list.

- To modify the events summaries sending time, set new time in the corresponding entry field. Events summaries will be delivered daily at the specified time.

- To disable (or enable, if disabled) the **Network Traffic Compression** option, deselect/select the corresponding check-box.

- To write event descriptions to a SQL database, select the corresponding check box.

- To view collected data from the Audit Archive, you can use the NetWrix Event Viewer tool. For more information on how to do this, refer to Section 10.3 Viewing Audit Data in NetWrix Event Viewer.

5. CONFIGURING REPORTS

The Event Log Manager functionality allows generating reports based on Microsoft SQL Server Reporting Services. The SSRS-based reports have the following advantages:

- You can use a wide variety of pre-defined report templates. Besides, these reports will help you stay compliant with different standards and regulations (GLBA, HIPAA, PCI, SOX).
- You can use different output formats for your reports, such as PDF, XLS, etc.

This chapter provides instructions on how to configure or modify the reports settings for your managed objects, and explains how to view reports. For detailed information, refer to the following sections:

- Specifying SQL Server Settings
- Uploading Report Templates to the SRS Server
- Assigning Permissions to View SSRS-Based Reports
- Viewing SSRS-Based Reports

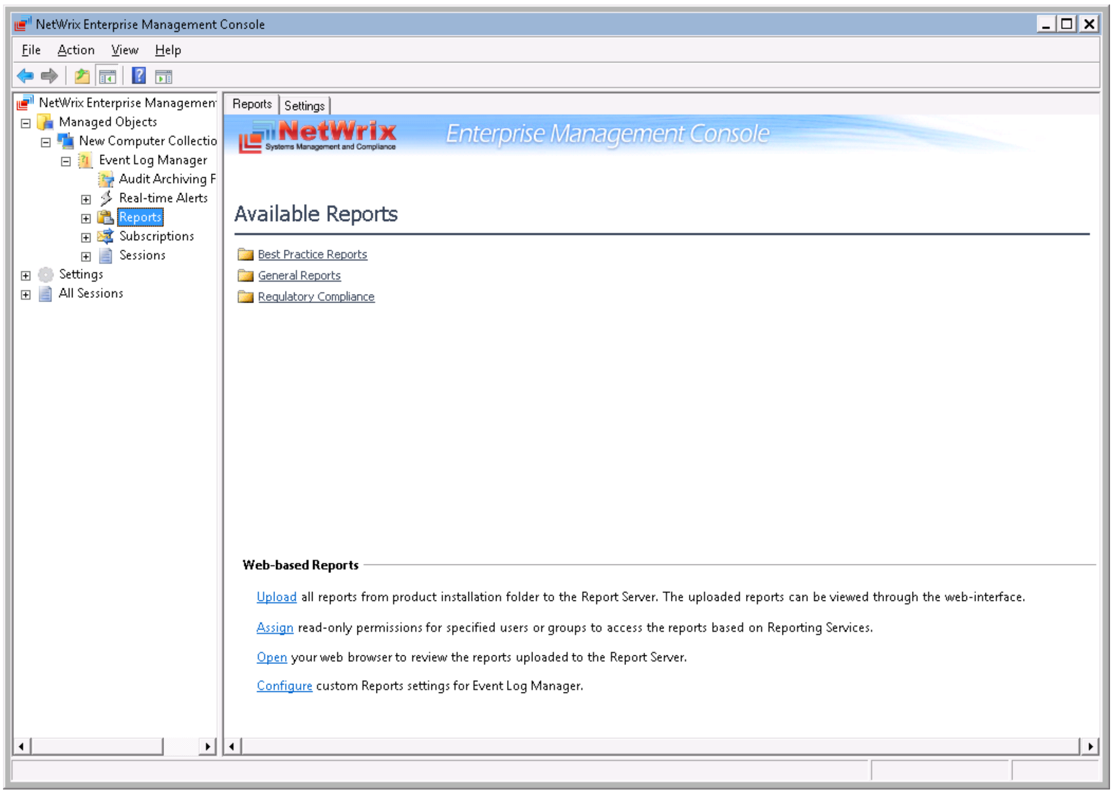
5.1. Specifying SQL Server Settings

To configure SQL Server settings for an existing Managed Object, perform the following procedure:

Procedure 6. To specify SQL Server settings

1. In NetWrix Enterprise Management Console, expand the **Managed Object** → **<your_managed_object>** → **Event Log Manager** node and select **Reports**. The following page will be displayed:

Figure 34: Reports Page



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

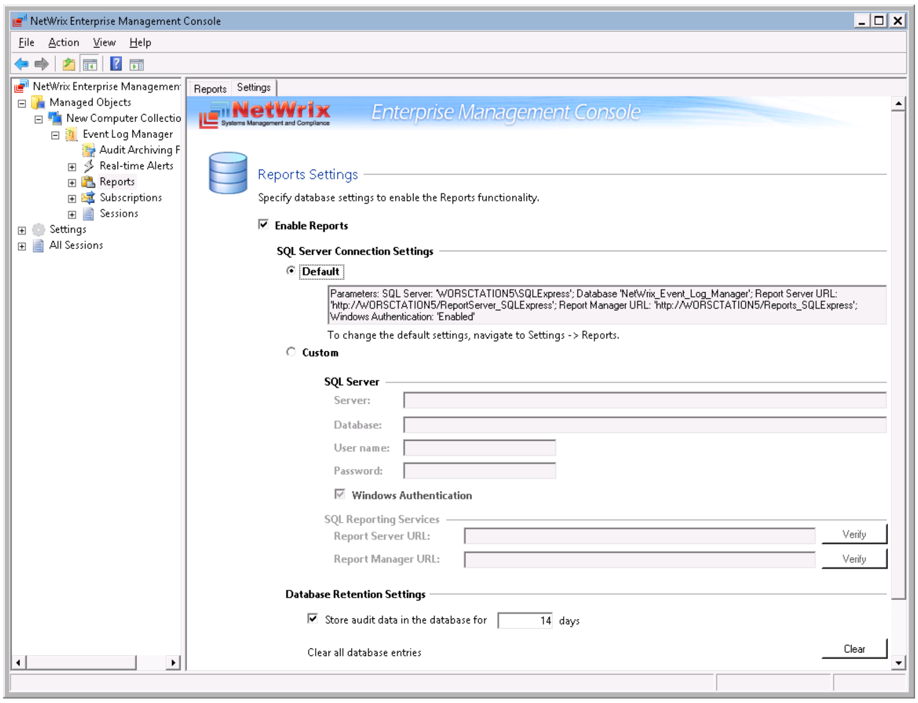
Assign read-only permissions for specified users or groups to access the reports based on Reporting Services.

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

Configure custom Reports settings for Event Log Manager.

2. In the right pane, click on **Configure** under **Web-based Reports**, or switch to the **Settings** tab. The following page will be displayed:

Figure 35: Reports Settings



Reports Settings

Specify database settings to enable the Reports functionality.

☑ Enable Reports

SQL Server Connection Settings

● Default

Parameters: SQL Server: 'WORSCTATION5\SQLExpress'; Database 'NetWrix_Event_Log_Manager'; Report Server URL: 'http://WORSCTATION5/ReportServer_SQLExpress'; Report Manager URL: 'http://WORSCTATION5/Reports_SQLExpress'; Windows Authentication: 'Enabled'

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

○ Custom

SQL Server

Server:

Database:

User name:

Password:

☑ Windows Authentication

SQL Reporting Services

Report Server URL: Verify

Report Manager URL: Verify

Database Retention Settings

☑ Store audit data in the database for 14 days

Clear all database entries Clear

3. Specify 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 Reports settings.
Server	Specify the name of an existing SQL Server instance where a database of audit data will be created.
Database	Specify the SQL database name.
User name	Specify a user to access the SQL Server. This user must belong to the target database owners (dbo) role.
Password	Specify a password to access the SQL Server.
Windows Authentication	Select this option if you want to use the default account (specified on Managed Object creation) 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.
Store audit data in the database for x days	Specify the retention period for collected data to be stored in the SQL database. **NOTE:** This value is set to 14 days by default. If you want to be able to view reports for a longer period in the past, change this value.

Clear all database entries	Click the **Clear** button if you want to delete all events from a SQL database.

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

5.2. Uploading Report Templates to the SRS Server

As part of the Reports feature, NetWrix Event Log Manager provides a set of pre-defined templates used to generate the most commonly required report types. These reports can be viewed in NetWrix Enterprise Management Console or in a web browser. In order to be able to view reports in a web browser, report templates must be uploaded to the SRS Server.

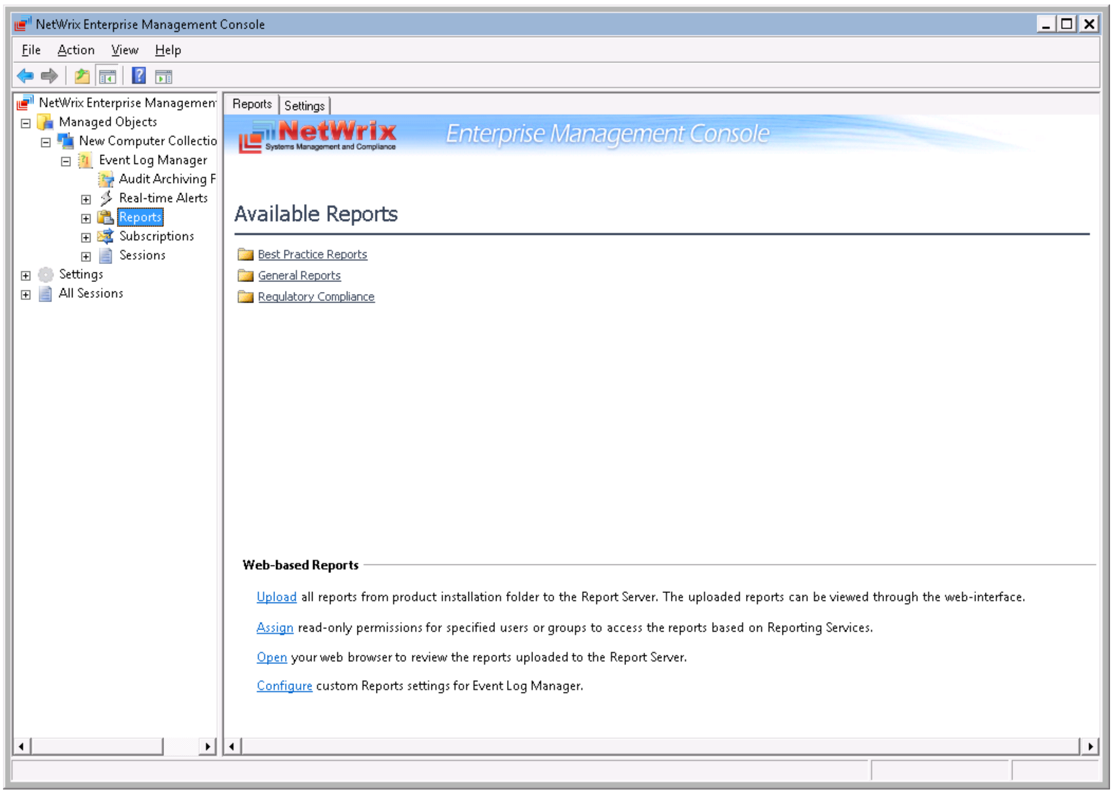
> **Note:** It is necessary to perform this operation only if you have not enabled the **Reports** feature when creating a Managed Object, otherwise report templates are uploaded to a SQL Server automatically.

To upload report templates, perform the following procedure:

Procedure 7. To upload report templates to the SRS server

1. In NetWrix Enterprise Management Console, expand the **Managed Object** → **<your_managed_object>** → **Event Log Manager** node and select **Reports**. The following page will be displayed:

Figure 36: Reports Page



Available Reports

Best Practice Reports
General Reports
Regulatory Compliance

Web-based Reports

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

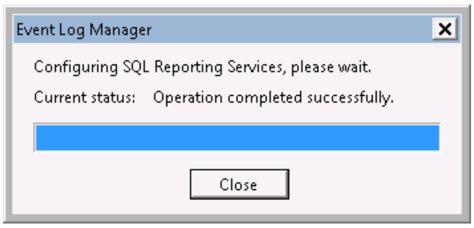
Assign read-only permissions for specified users or groups to access the reports based on Reporting Services.

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

Configure custom Reports settings for Event Log Manager.

2. Click **Upload** under **Web-based Reports**. The system will upload all report templates to the SRS server and display the following confirmation message when the operation is completed:

Figure 37: Report Templates Upload Confirmation



Event Log Manager

Configuring SQL Reporting Services, please wait.

Current status: Operation completed successfully.

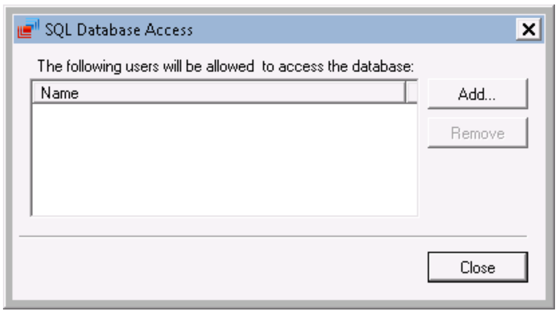
5.3. Assigning Permissions to View SSRS-Based Reports

Your situation may require that different users in your organization have access to SSRS-based reports. By default, SSRS-based reports can only be accessed by domain administrators. To grant other users access to these reports, perform the following procedure:

Procedure 8. To assign permissions to view SSRS-based reports

1. In the Reports page (see Figure 36: Reports Page), click on **Assign** under **Web-based Reports**. The following dialog will be displayed:

Figure 38: 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 domain. Then click **OK**. The selected users will now be able to view SSRS-based reports.

5.4. Viewing SSRS-Based Reports

You can view SSRS-based reports in a web browser. Click **Open** under **Web-based Reports** in the **Reports** page. Your default browser will be opened, and you will see the Report Manager home page. For further instructions and reports examples, refer to Section 11.2.2 Viewing Reports in a Web Browser.

6. Configuring Subscriptions to Reports

In NetWrix Event Log Manager, you can configure automatic report delivery by creating a subscription. Reports will be generated automatically and delivered to the specified recipients. You can apply various filters to your reports and choose their output format. This chapter provides detailed step-by-step instructions on how to:

- Configure a subscription
- Modify a subscription

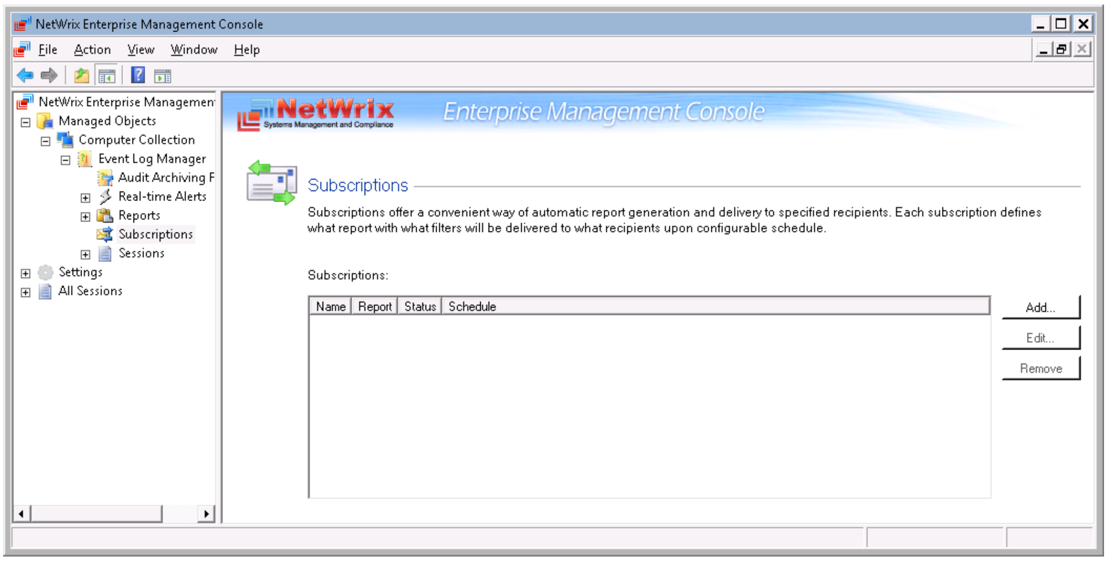
6.1. Configuring a Subscription

To create a subscription, perform the following procedure:

Procedure 9. To create a subscription

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<your_managed_object>** → **Event Log Manager** node and select **Subscriptions**. The following page will be displayed:

Figure 39: Subscriptions Page



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:

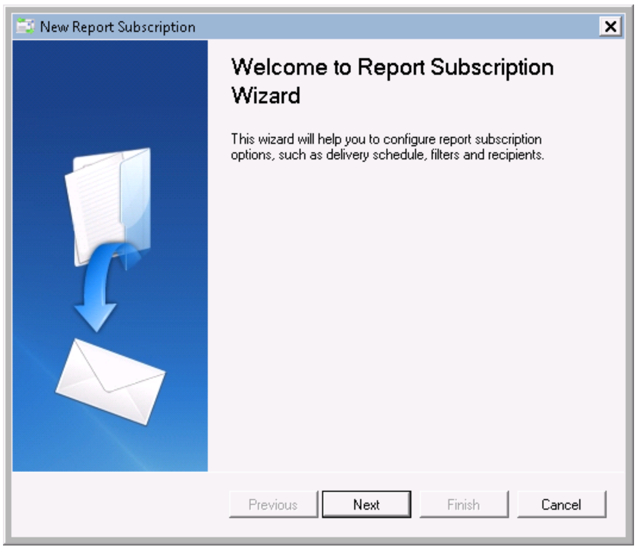
Name	Report	Status	Schedule

2. Click the **Add** button to start the Report Subscription wizard:

Note: Alternatively, you can expand the **Reports** node, select the report you want to subscribe to, and click the **Subscribe** button in the right pane.

Suggestions or comments about this document? www.netwrix.com/feedback

Figure 40: New Report Subscription Wizard: Start Page

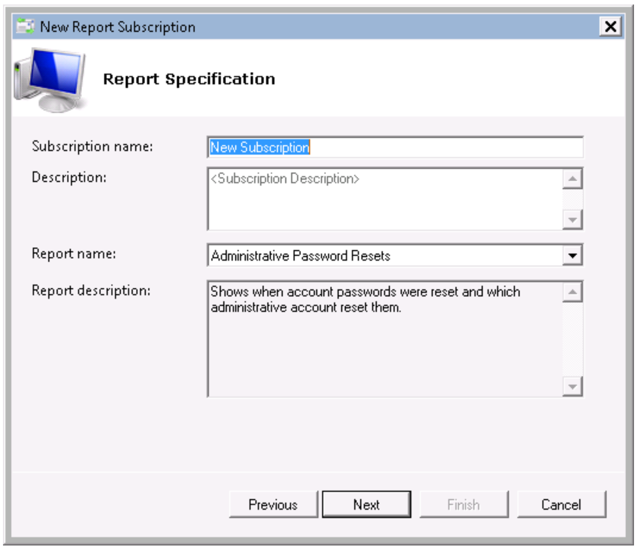


Welcome to Report Subscription Wizard

This wizard will help you to configure report subscription options, such as delivery schedule, filters and recipients.

3. Click **Next**. When connection with the Report Server is established, the following dialog will be displayed:

Figure 41: New Report Subscription Wizard: Report Specification



Subscription name: New Subscription

Description: <Subscription Description>

Report name: Administrative Password Resets

Report description: Shows when account passwords were reset and which administrative account reset them.

Specify the following parameters:

Table 7: Subscription Settings

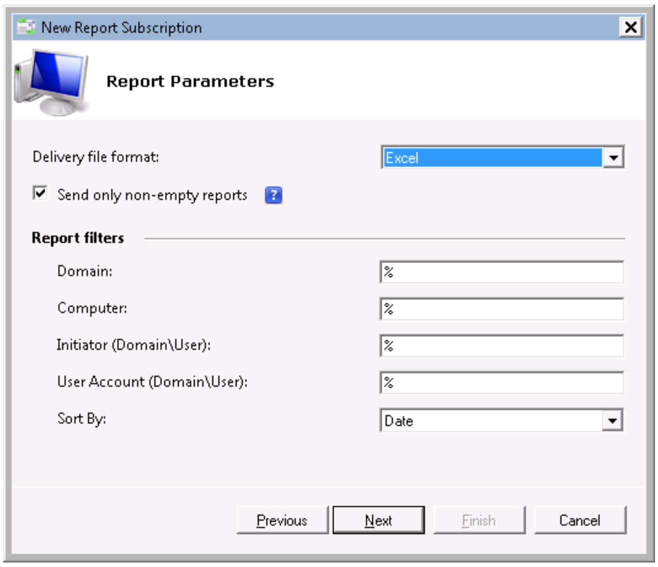
Parameter	Description
Subscription Name	Specify subscription name (this name will be displayed in NetWrix Enterprise Management Console under the **Subscriptions** node).
Description	Enter subscription description (optional).
Report name	Select the report that you want to subscribe to from the drop-down list. **NOTE:** If you start the Report Subscription wizard from a specific report, this field will be filled in automatically.

Click **Next** to proceed.

4. On the next step, you must specify the report recipients. Click the **Add** button and specify the email address(es) where the report must be delivered. It is recommended to click the **Verify** button. The system will send a test message to the specified email address(es) and will inform you if any problems are detected. Then click **Next** to continue.

5. On the next step, you must specify the report parameters, which may differ depending on the selected report type:

Figure 42: New Report Subscription Wizard: Report Parameters



Delivery file format: Excel

☑ Send only non-empty reports

Report filters

Domain: %

Computer: %

Initiator (Domain\User): %

User Account (Domain\User): %

Sort By: Date

6. On the next step, specify the report delivery schedule:

   - on a daily basis (reports will be delivered at a specified interval in days at 3:00 AM);
   - on a weekly basis (reports will be delivered on specified days of a week at 3:00 AM);
   - on a monthly basis (reports will be delivered in specified months on a selected date at 3:00 AM).

7. Click **Next** to continue. On the last step, review your settings and click **Finish**. A new subscription will appear under the **Subscriptions** node in the left pane.

6.2. Modifying a Subscription

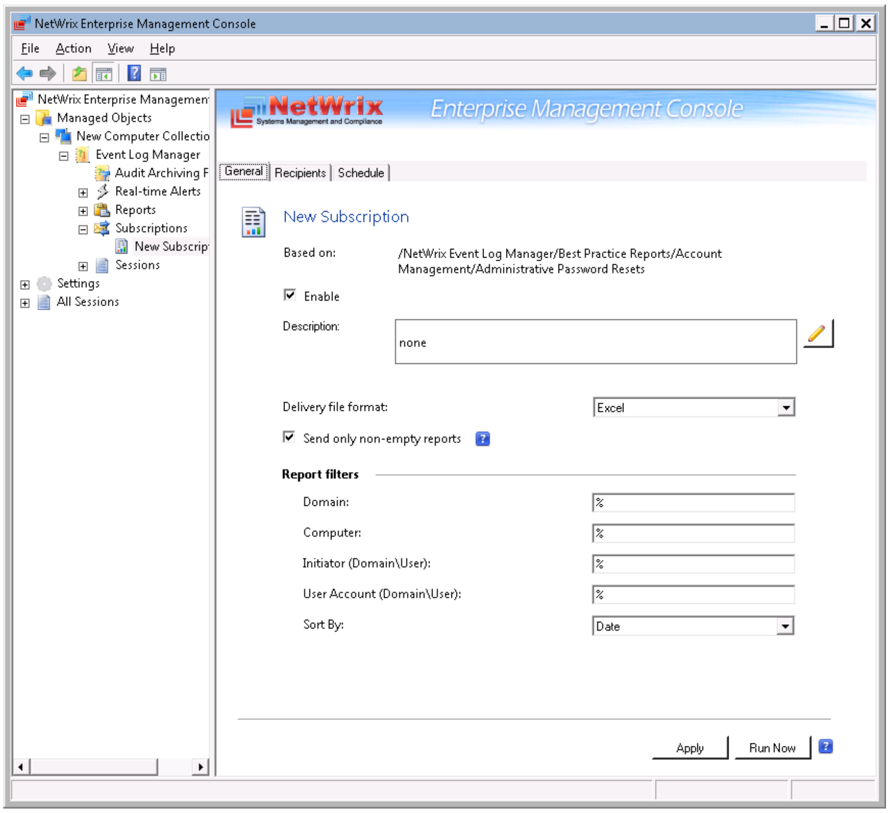
If later you need to modify an existing subscription, perform one of the following procedures:

- Procedure 10 To modify subscription general settings
- Procedure 11 To modify a report recipients list
- Procedure 12 To modify a report delivery schedule

Procedure 10. To modify subscription general settings

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<your_managed_object>** → **Event Log Manager** → **Subscriptions** node and select the subscription that you want to modify. The **General** tab of the subscription page will be displayed:

Figure 43: Subscriptions Page: General Tab



New Subscription

Based on: /NetWrix Event Log Manager/Best Practice Reports/Account Management/Administrative Password Resets

☑ Enable

Description: none

Delivery file format: Excel

☑ Send only non-empty reports

Report filters

Domain: %

Computer: %

Initiator (Domain\User): %

User Account (Domain\User): %

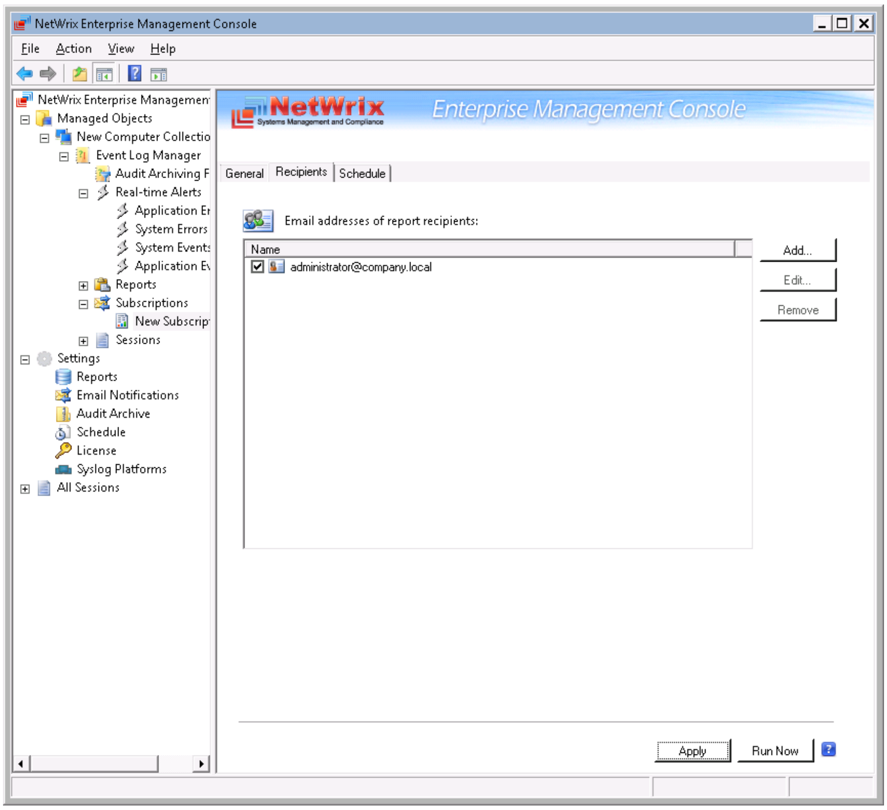
Sort By: Date

2. Modify the required parameters.
3. Click **Apply** to save the changes.

Procedure 11. To modify a report recipients list

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<your_managed_object>** → **Event Log Manager** → **Subscriptions** node, select the subscription that you want to modify and open the **Recipients** tab:

Figure 44: Subscription Page: Recipients Tab



Email addresses of report recipients:

Name
☑ administrator@company.local

2. Perform one of the following operations if necessary:

   - To add an email address to the Report Recipients list, click the **Add** button. Specify the email address you want to add and click **OK**. To check the correctness of 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.

   - To modify an email address in the Report Recipients list, select it from the list and click the **Edit** button. Edit the address and click **OK**.

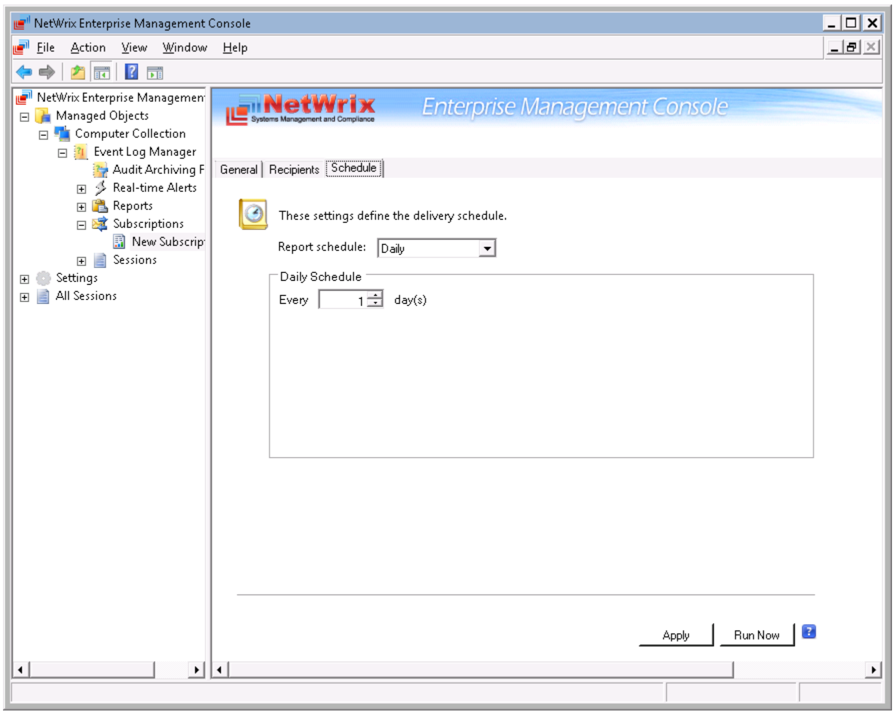
   - To remove an email address from the Report Recipients list, select it from the list and click the **Remove** button. The selected address will be removed from the list.

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

Procedure 12. To modify a report delivery schedule

1. In NetWrix Enterprise Management Console, expand the **Managed Objects** → **<your_managed_object>** → **Event Log Manager** → **Subscriptions** node, select the subscription that you want to modify and open the **Schedule** tab:

Figure 45: Subscription Page: Schedule Tab



These settings define the delivery schedule.

Report schedule: Daily

Daily Schedule

Every 1 day(s)

2. Modify the report delivery schedule if necessary, and click **Apply** to save the changes.

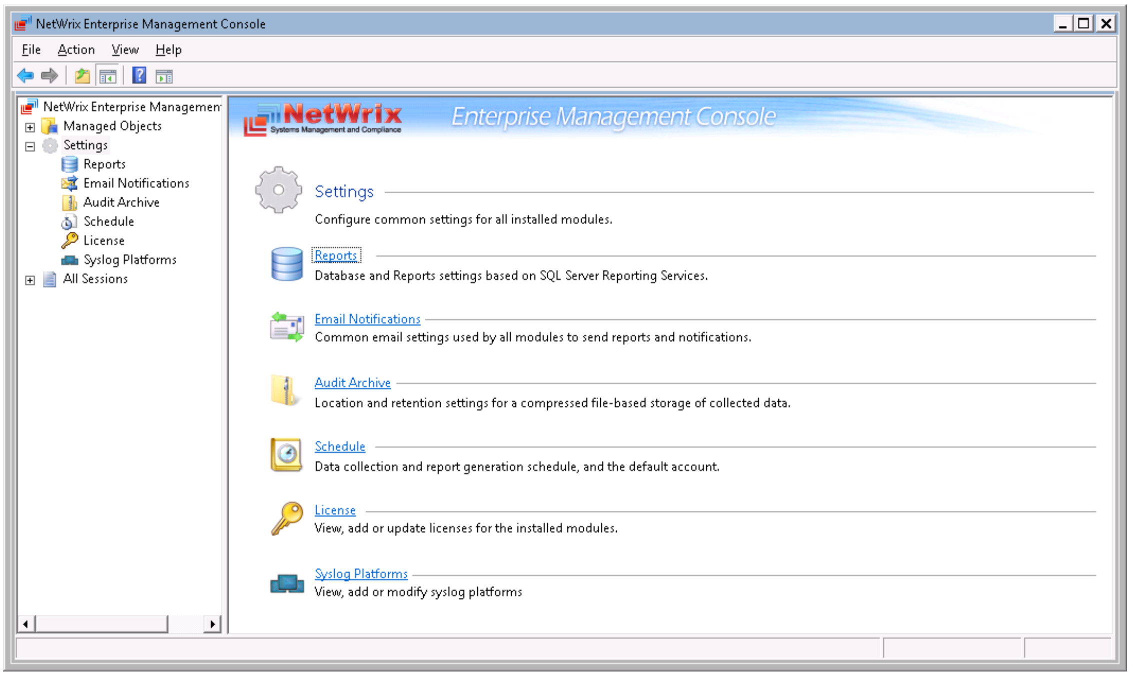
7. CONFIGURING GLOBAL SETTINGS

NetWrix Enterprise Management Console provides a convenient interface for configuring 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 for the NetWrix Event Log Manager module enabled for this object, refer to Chapter 4 Configuring Managed Objects above.

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

Figure 46: 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.

Syslog Platforms
View, add or modify syslog platforms

The following settings can be configured:

- Reports Settings
- Email Notifications Settings
- Audit Archive Settings
- Default Data Processing Account
- License Settings
- Configuring the Syslog Platform Settings

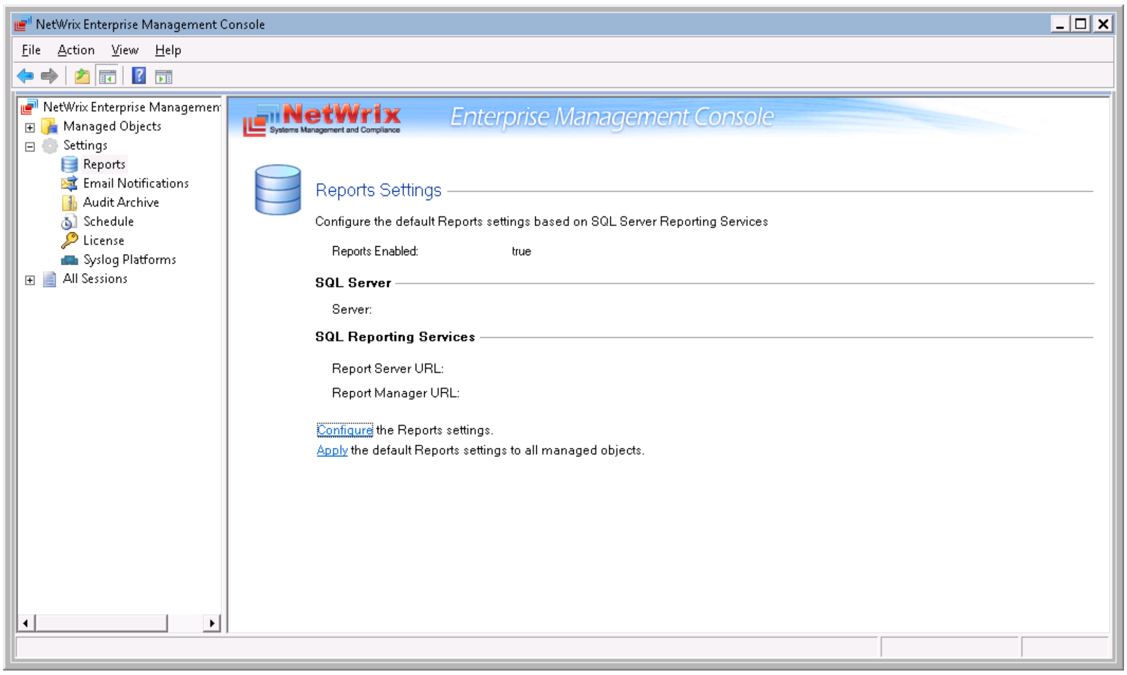
7.1. Configuring the Reports Settings

The **Reports** option allows configuring the reports settings. To do this, perform the following procedure:

Procedure 13. To configure the Reports settings

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

Figure 47: Reports Settings Page



Reports Settings

Configure the default Reports settings based on SQL Server Reporting Services

Reports Enabled: true

SQL Server

Server:

SQL Reporting Services

Report Server URL:

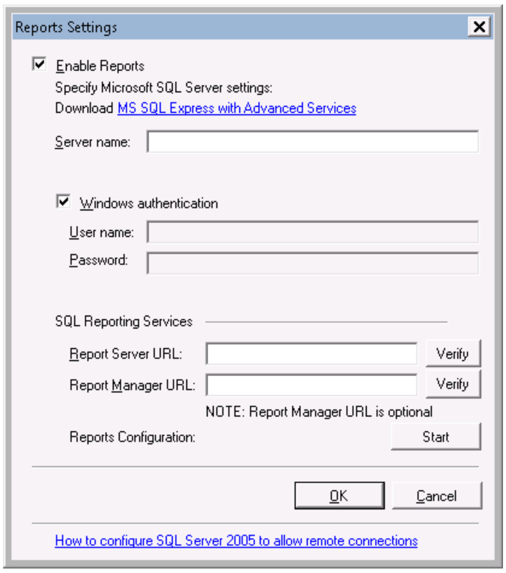
Report Manager URL:

Configure the Reports settings.

Apply the default Reports settings to all managed objects.

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

Figure 48: The Reports Settings Dialog



☑ Enable Reports

Specify Microsoft SQL Server settings:

Download MS SQL Express with Advanced Services

Server name:

☑ Windows authentication

User name:

Password:

SQL Reporting Services

Report Server URL:

Report Manager URL:

NOTE: Report Manager URL is optional

Reports Configuration:

How to configure SQL Server 2005 to allow remote connections

3. Configure the following settings if necessary:

Table 8: Reports Settings

Parameter	Description
Enable Reports	Select this check box to enable Reports for all Managed Objects.
Server name	Specify the name of an existing SQL Server instance where a database of audit data will be created.
Windows authentication	Select this option if you want to use the default account to access the SQL database.
User name	Specify a user name to access the SQL Server. **NOTE**: This user must belong to target database owners (dbo) role.

Password	Specify a password to access the SQL Server.
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 automatically install and configure Microsoft SQL 2005 Express with Advanced Services.

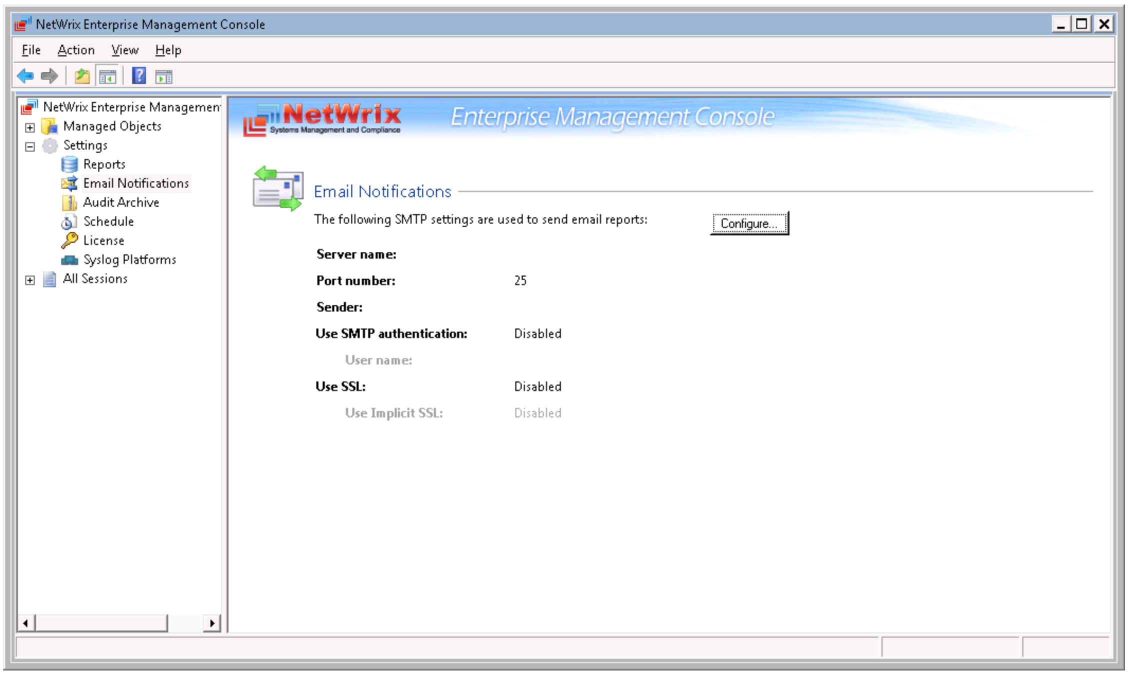
7.2. Configuring the Email Notifications Settings

The **Email Settings** option allows configuring the SMTP settings used to deliver events summaries and reports to the specified recipients. To do this, perform the following procedure:

Procedure 14. To configure the email settings

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

Figure 49: Email Notifications Page



Email Notifications

The following SMTP settings are used to send email reports:

Server name:

Port number: 25

Sender:

Use SMTP authentication: Disabled

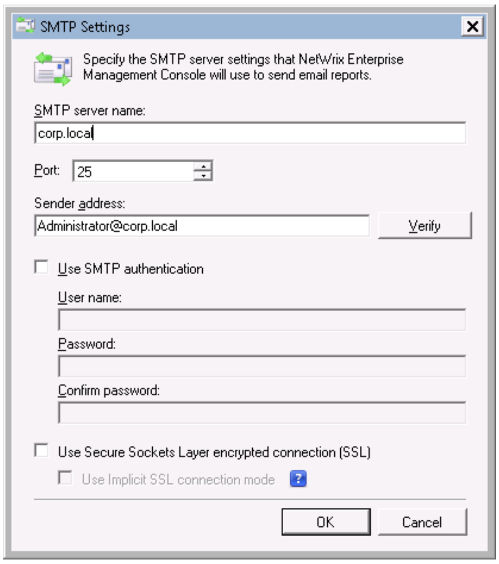
User name:

Use SSL: Disabled

Use Implicit SSL: Disabled

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

Figure 50: SMTP Settings



SMTP Settings

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

SMTP server name: corp.local

Port: 25

Sender address: Administrator@corp.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 if necessary. For email settings detailed description refer to Table 2: Email Settings Parameters.

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

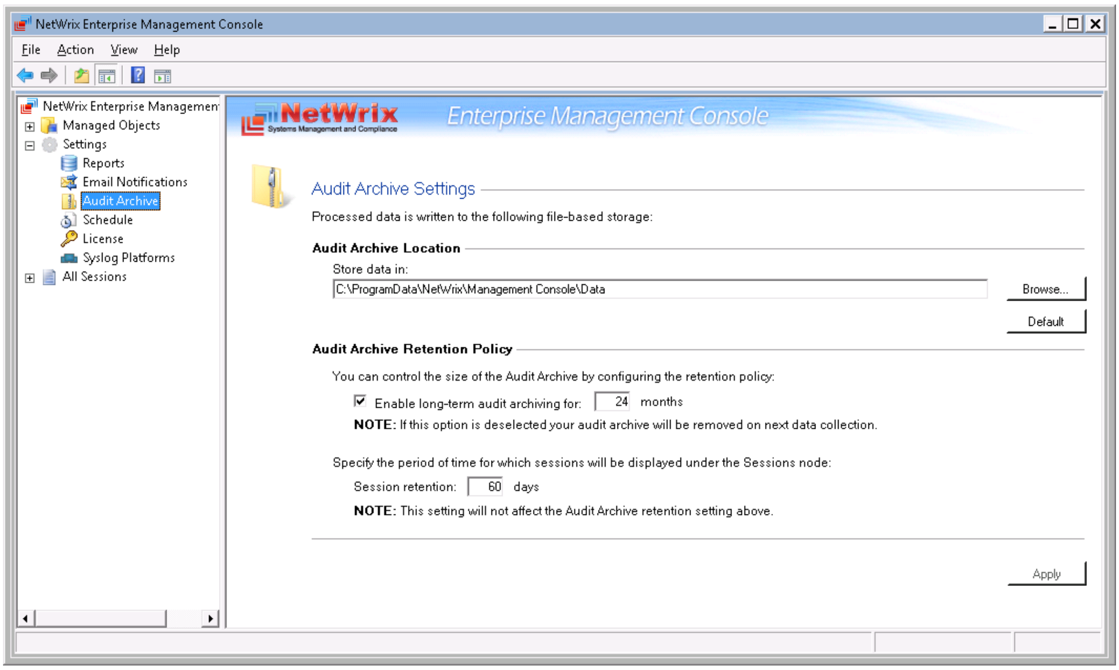
7.3. Configuring Audit Archive Settings

This option allows configuring the Audit Archive settings. To configure these settings, perform the following procedure:

Procedure 15. To configure the Audit Archive settings

1. In NetWrix Enterprise Management Console, expand the **Settings** node and select the **Audit Archive** option. Alternatively, you can expand the **Settings** node and select **Audit Archive** in the right pane. The following page showing the current audit archive settings will be displayed:

Figure 51: Audit Archive Settings Page



Audit Archive Settings

Processed data is written to the following file-based storage:

Audit Archive Location

Store data in: C:\ProgramData\NetWrix\Management Console\Data

Audit Archive Retention Policy

You can control the size of the Audit Archive by configuring the retention policy:

☑ Enable long-term audit archiving for: 24 months

NOTE: If this option is deselected your audit archive will be removed on next data collection.

Specify the period of time for which sessions will be displayed under the Sessions node:

Session retention: 60 days

NOTE: This setting will not affect the Audit Archive retention setting above.

2. Modify the following settings if necessary:

    - Audit Archive Location: specify the path to the folder where your audit data must be stored.
    - Audit Archive Retention Policy: specify the period of time for which audit data must be stored, and the session retention period.

    Note: The session retention period value does not affect the audit archive retention period; it merely determines the period of time for which sessions (i.e. information about daily data collection) will be displayed under the **Sessions** node.

7.4. Configuring the Default Data Processing Account

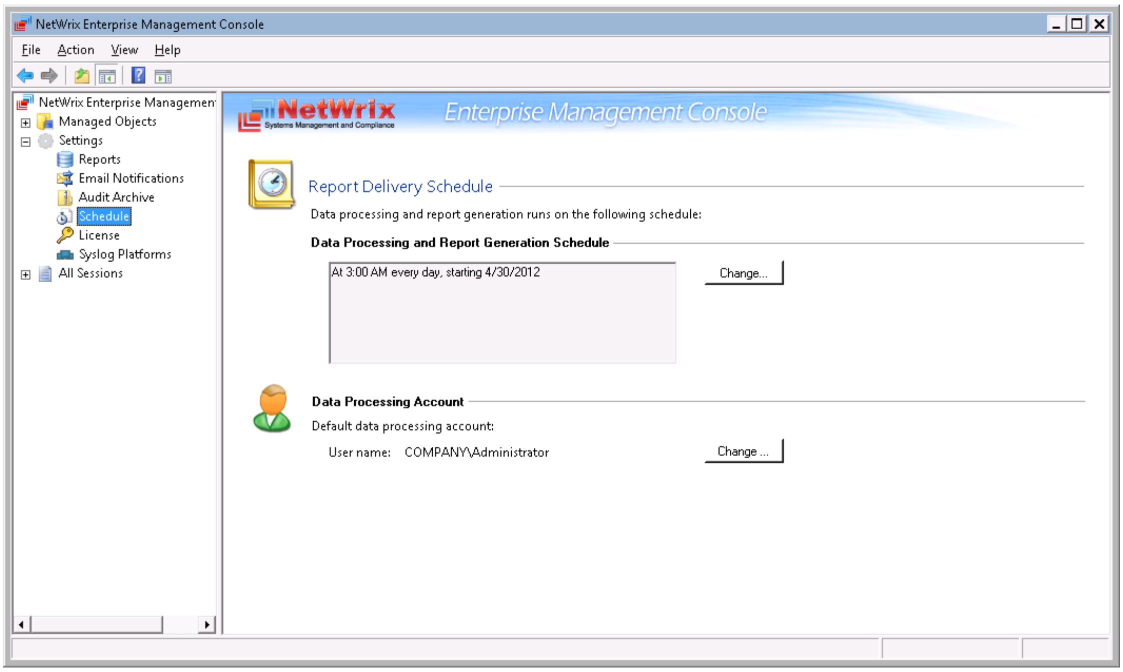
To configure the default data processing account, perform the following procedure:

Procedure 16. To configure the default data processing account

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

    Note: Disregard the Data Processing and Report Generation Schedule setting. These settings refer to other NetWrix products and do not affect the NetWrix Event Log Manager functionality.

Figure 52: Report Delivery Schedule Settings Page



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 4/30/2012

Data Processing Account

Default data processing account:

User name: COMPANY\Administrator

2. To modify the default data processing account, click the **Change** button under **Data Processing Account**. In the dialog that opens, specify the default account and its credentials and click **OK**.

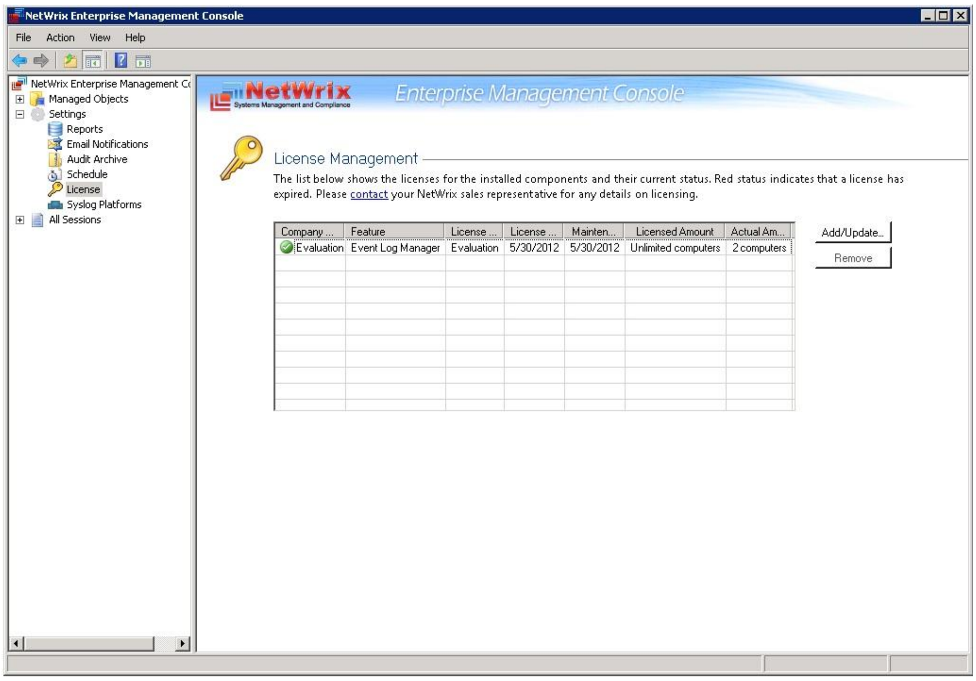
7.5. Configuring the License Settings

The **License** option allows viewing your current licenses for the installed NetWrix products, updating them and adding new licenses. To configure your licenses, perform the following procedure:

Procedure 17. To configure licenses

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

Figure 53: License Management Page



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 Amount	Actual Am...
✓ Evaluation	Event Log Manager	Evaluation	5/30/2012	5/30/2012	Unlimited computers	2 computers

2. Perform one of the following operations if necessary:

- To add/update your licenses, click the **Add/Update** button. In the dialog that opens, specify your company name, your license count and the license codes (separated by commas or semi-colons).

Note: You can only add multiple licenses at the same time if they have the same license count. Otherwise, add them separately.

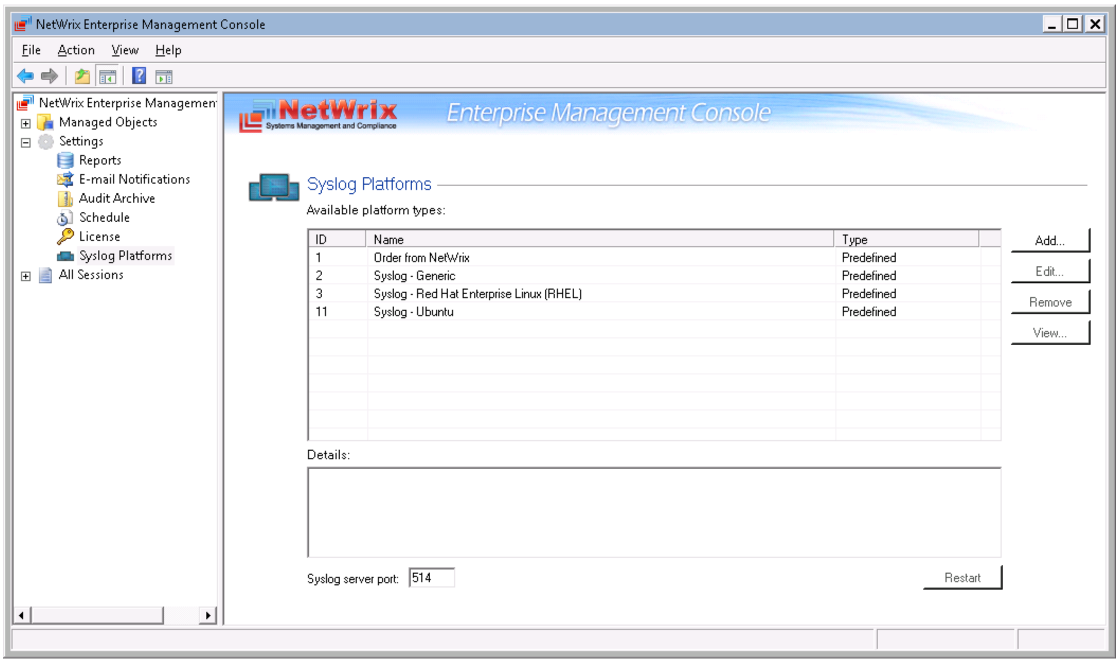
- To remove a license, select it from the list and click the **Remove** button. Then click **Yes** in the confirmation dialog.

7.6. Configuring the Syslog Platform Settings

The **Syslog** option allows creating and configuring Syslog-based platforms that can be subsequently selected as item types for your Managed Objects.

To display a list of currently available Syslog-based platforms, in NetWrix Enterprise Management Console expand the **Settings** node and select the **Syslog Platforms** option. The following page will be displayed:

Figure 54: Syslog Platforms Page



Syslog Platforms

Available platform types:

ID	Name	Type
1	Order from NetWrix	Predefined
2	Syslog - Generic	Predefined
3	Syslog - Red Hat Enterprise Linux (RHEL)	Predefined
11	Syslog - Ubuntu	Predefined

Details:

Syslog server port: 514

There are three predefines platform types: Generic, Red Hat Enterprise Linux 5, and Ubuntu.

The following operations are supported:

- Order a Syslog-based platform from NetWrix if the predefined platforms do not cover your needs. To do this, select **Order from NetWrix** and click the link under **Details**.
- Add a Syslog-based platform. To do this, click the **Add** button. For detailed instructions, refer to Procedure 18 To create a Syslog-based platform.
- Edit a Syslog-based platform. To do this, click the **Edit** button and modify the necessary parameters.

  Note: You cannot edit a predefined platform. If you try to edit it, a copy of this platform will be created, which can be modified.

- Remove a Syslog-based platform. To do this, select a platform and click the **Remove** button.

  Note: You cannot remove a predefined platform.

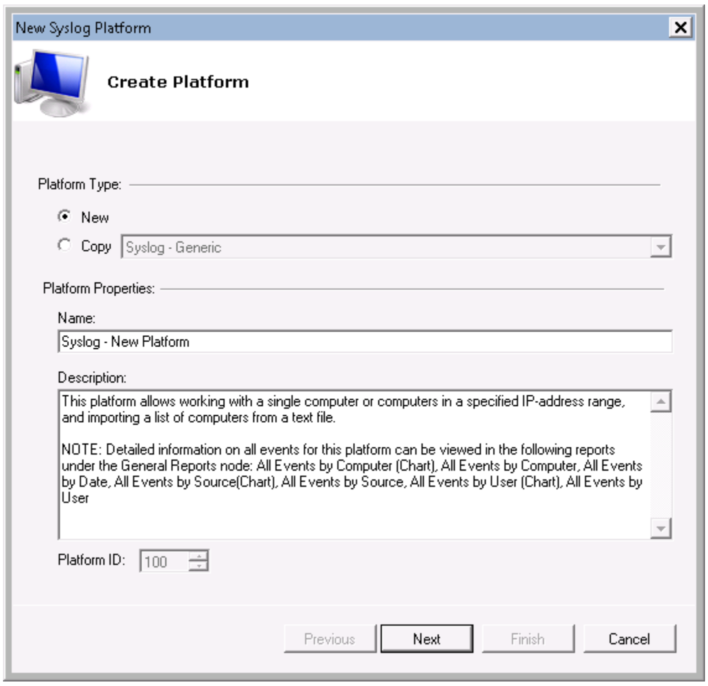
- View platform rules. To do this, select a platform and click **View**.
- Change a Syslog server port. To do this, type a new port number and click the **Restart** button.

To create a Syslog-based platform, perform the following procedure:

Procedure 18. To create a Syslog-based platform

1. On the Syslog Platforms page click the **Add** button. The following dialog will be displayed:

Figure 55: New Syslog Platform Wizard: Creating a Platform



New Syslog Platform

Create Platform

Platform Type:

● New

○ Copy Syslog - Generic

Platform Properties:

Name: Syslog - New Platform

Description:

This platform allows working with a single computer or computers in a specified IP-address range, and importing a list of computers from a text file.

NOTE: Detailed information on all events for this platform can be viewed in the following reports under the General Reports node: All Events by Computer (Chart), All Events by Computer, All Events by Date, All Events by Source(Chart), All Events by Source, All Events by User (Chart), All Events by User

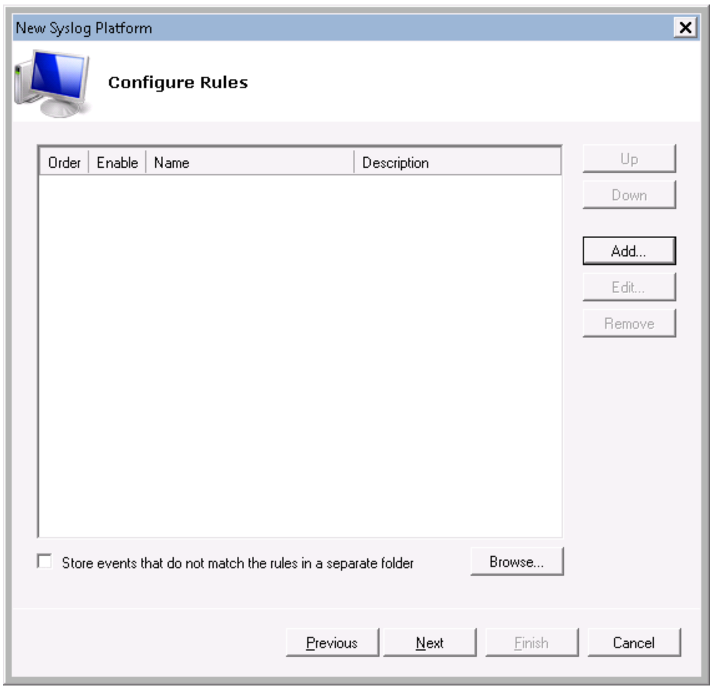
Platform ID: 100

2. Specify platform type. By selecting the **New** option, you can create a new platform and define its rules. Alternatively, you can select the **Copy** option, and create a platform based on a predefined platform, thus inheriting its rules (which you can edit).

3. Specify platform name and description (optional).

4. Click **Next**. The following page will open:

Figure 56: New Syslog Platform Wizard: Configuring Rules



New Syslog Platform

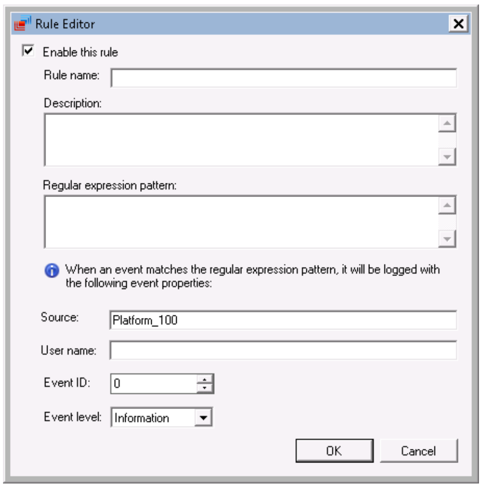
Configure Rules

Order	Enable	Name	Description

□ Store events that do not match the rules in a separate folder

5. To add an events processing rule click the **Add** button. The following dialog will be displayed:

Figure 57: Syslog Rules Editor



Rule Editor

☑ Enable this rule

Rule name:

Description:

Regular expression pattern:

When an event matches the regular expression pattern, it will be logged with the following event properties:

Source: Platform_100

User name:

Event ID: 0

Event level: Information

6. Specify the following parameters:

Table 9: Syslog Rules Settings

Parameter	Description
Enable this rule	Make sure that this option is selected.
Rule name	Specify rule name.
Description	Specify rule description (optional).
Regular expression pattern	Specify a pattern, according to which events will be collected. When an event matches this pattern, this event will be logged.
The rows below contain information that will be added to a Syslog event if it matches a specified pattern. This information can be used to filter events and sort them by.	
Source	Specify the name of a source. It can be any word that will help you identify the platform where an event was generated.
User name	Specify the number of a capturing group which defines a user name in a pattern in the following format: %Capturing_Group_Number. If needed, you can add more information, for example: Doman_Name\%Capturing_Group_Number. **NOTE**: the right Capturing_Group_Number can be calculated if you enumerate capturing groups in a pattern starting from 0.
Event ID	Specify a number which will be added to an event as its ID.
Event level	Specify the event level.

7. Click **OK** to save the changes.

8. In the **Configure rules** dialog, you can edit or remove created rules. Also, you can change the order, in which rules will be applied to collected events.

9. To store events that do not match any of the rule patterns, select the corresponding check box.

10. Click **Next**.

11. On the last step, review your platform settings and click **Finish**.

The newly created Syslog-based platform will appear under the **Available Platform Types.**

> **Note:** To view reports for the predefined platforms, there are default report templates located in **Reports → Best Practice Reports → Syslog**. To view reports for custom platforms, you can use report templates located in **Reports → General Reports.**

8. CONFIGURING EVENTS SUMMARY OPTIONS

NetWrix Event Log Manager allows configuring the events summary settings via the .txt configuration files located in the program installation folder. The following configuration files are provided:

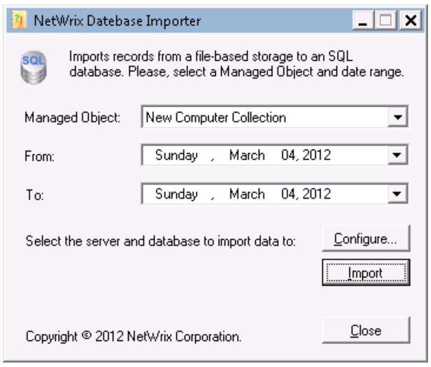
- mailTemplate.txt: this file contains the events summary template. Edit it to modify the message template.
- omitErrorList.txt: this file contains a list of errors' descriptions. If you want to exclude a specific error that can occur during data collection from events summaries (for an example message, see Figure 69: Events Summary with the Error), specify the error's text in the file. The file structure is as follows:
    - Lines that start with the # sign are treated as comments and are ignored.
    - Wildcards are supported.
    - Each entry must be a separate line.

9. Importing Audit Data

NetWrix Database Importer is a tool intended for importing data from the Audit Archive to a SQL database. You can use it to manually import events to a SQL database if you only configured to write events to the Audit Archive, or for data recovery in case a SQL database was corrupted.

To launch NetWrix Database Importer, navigate to **Start → All Programs → NetWrix → Event Log Manager → Advanced Tools → DB Importer**. NetWrix Database Importer will be opened:

Figure 58: NetWrix Database Importer



NetWrix Datebase Importer

Imports records from a file-based storage to an SQL database. Please, select a Managed Object and date range.

Managed Object: New Computer Collection

From: Sunday , March 04, 2012

To: Sunday , March 04, 2012

Select the server and database to import data to:

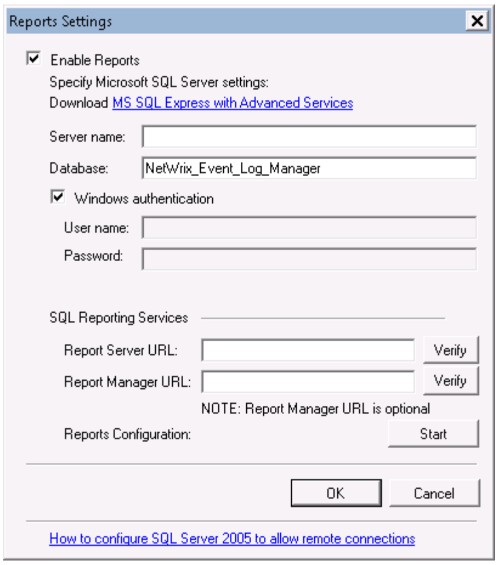
Copyright © 2012 NetWrix Corporation.

You can import data for a specified period of time separately for each Managed Object.

> **Note:** When importing data, make sure that the date range you specified does not exceed the retention period for the Audit Archive and the SQL database, otherwise not all of the data will be imported.

Also, you can configure Reports settings by clicking the **Configure** button:

Figure 59: The Reports Settings Dialog



Reports Settings

☑ Enable Reports

Specify Microsoft SQL Server settings:

Download MS SQL Express with Advanced Services

Server name:

Database: NetWrix_Event_Log_Manager

☑ Windows authentication

User name:

Password:

SQL Reporting Services

Report Server URL:

Report Manager URL:

NOTE: Report Manager URL is optional

Reports Configuration:

How to configure SQL Server 2005 to allow remote connections

> **Note:** For a description of the Reports parameters, refer to Table 3: Reports Parameters.

You can configure the settings manually, or use the Reports Configuration wizard. To start the wizard, click the **Start** button.

10. DATA COLLECTION

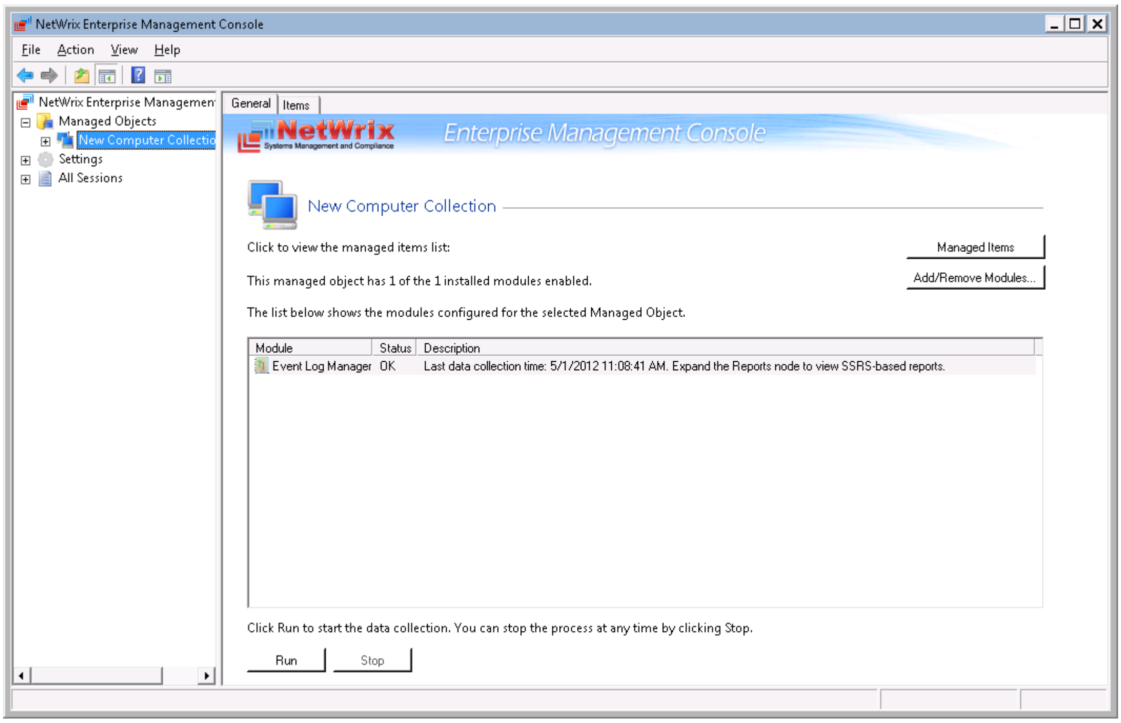
NetWrix Event Log Manager collects audit data, stores these data in the Audit Archive and/or an SQL database and sends events summaries (at 3:00 AM every day by default).

> **Note:** For instructions on how to change the events summaries delivery schedule, refer to Procedure 5 To modify the Event Log Manager settings.

If later you need to view all audit data collected within a specific period, you can use the NetWrix Event Viewer tool. For more information, refer to Section 10.3 Viewing Audit Data in NetWrix Event Viewer.

To manually generate an events summary, in NetWrix Enterprise Management Console expand the **Managed Objects** node, select your Managed Object and click the **Run** button in the right pane:

Figure 60: Computer Collection Page



Click to view the managed items list:

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

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

Module	Status	Description
Event Log Manager	OK	Last data collection time: 5/1/2012 11:08:41 AM. Expand the Reports node to view SSRS-based reports.

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

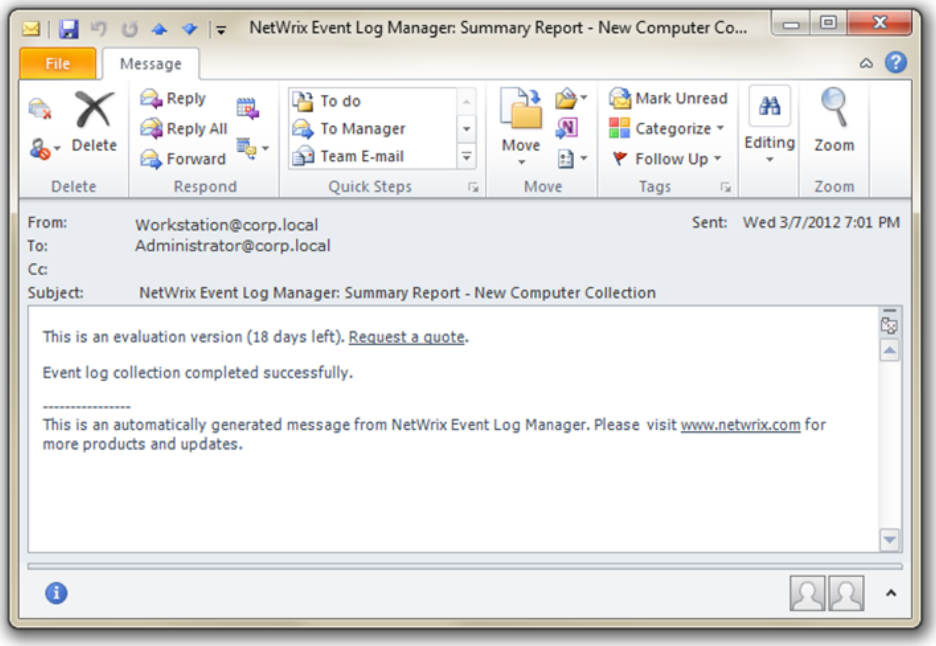
10.1. Data Collection Workflow

A typical data collection workflow is as follows:

1. When a new Managed Object is added, NetWrix Event Log Manager starts collecting events from monitored computers according to the specified filters.

2. After all currently available events are collected, an initial events summary is sent to the specified recipient(s):

Figure 61: Events Summary



From: Workstation@corp.local
To: Administrator@corp.local
Cc:
Subject: NetWrix Event Log Manager: Summary Report - New Computer Collection
Sent: Wed 3/7/2012 7:01 PM

This is an evaluation version (18 days left). Request a quote.

Event log collection completed successfully.

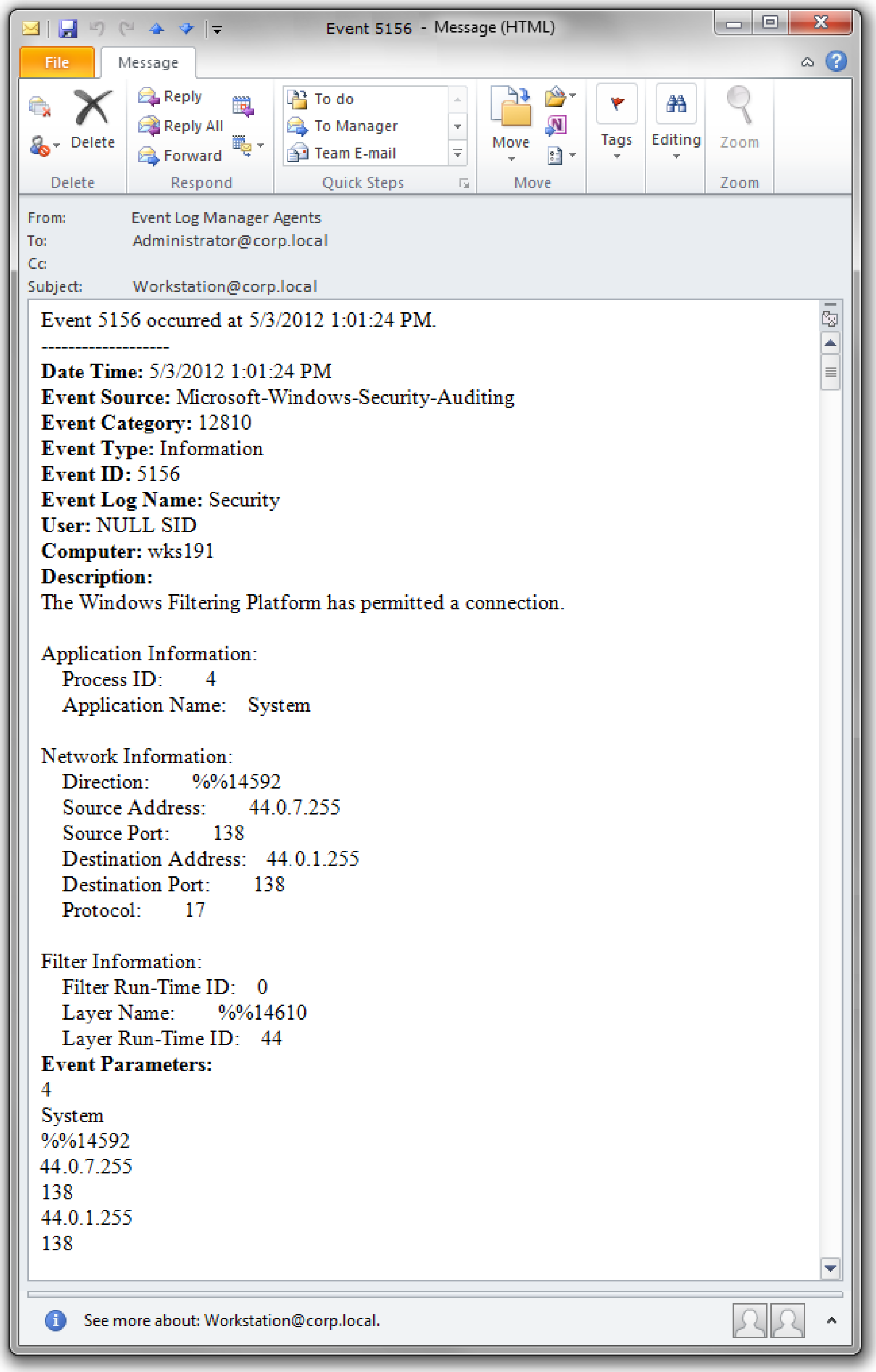
This is an automatically generated message from NetWrix Event Log Manager. Please visit www.netwrix.com for more products and updates.

3. Events are written to the Audit Archive and/or a SQL database.

   Note: If writing to a SQL database is impossible due to database inaccessibility, failure, etc., SQL data will be stored in a temporary repository until the issue is resolved. Depending on the number of events the product collects, the temporary repository size can grow very fast, so it is recommended to locate it on a disk with enough free space available. You can change the location of a temporary repository by modifying the **HKEY_LOCAL_MACHINE\ SOFTWARE\ NetWrix\ Event Log Manager\ Database Settings\ ImportToDbPath** key value (**HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ NetWrix\ Event Log Manager\ Database Settings\ ImportToDbPath** for 64-bit OS).

4. If during data collection an event is detected that triggers an alert, an email notification is sent to the specified recipients:

Figure 62: Example Alert Notification



From: Event Log Manager Agents
To: Administrator@corp.local
Cc:
Subject: Workstation@corp.local

Event 5156 occurred at 5/3/2012 1:01:24 PM.

Date Time: 5/3/2012 1:01:24 PM
Event Source: Microsoft-Windows-Security-Auditing
Event Category: 12810
Event Type: Information
Event ID: 5156
Event Log Name: Security
User: NULL SID
Computer: wks191
Description:
The Windows Filtering Platform has permitted a connection.

```
Application Information:
    Process ID:        4
    Application Name:    System

Network Information:
    Direction:        %%14592
    Source Address:       44.0.7.255
    Source Port:        138
    Destination Address:    44.0.1.255
    Destination Port:       138
    Protocol:        17

Filter Information:
    Filter Run-Time ID:    0
    Layer Name:       %%14610
    Layer Run-Time ID:    44
```

Event Parameters:
4
System
%%14592
44.0.7.255
138
44.0.1.255
138

See more about: Workstation@corp.local.

A real-time alert contains the following information:

Table 10: Real-Time Alert Fields

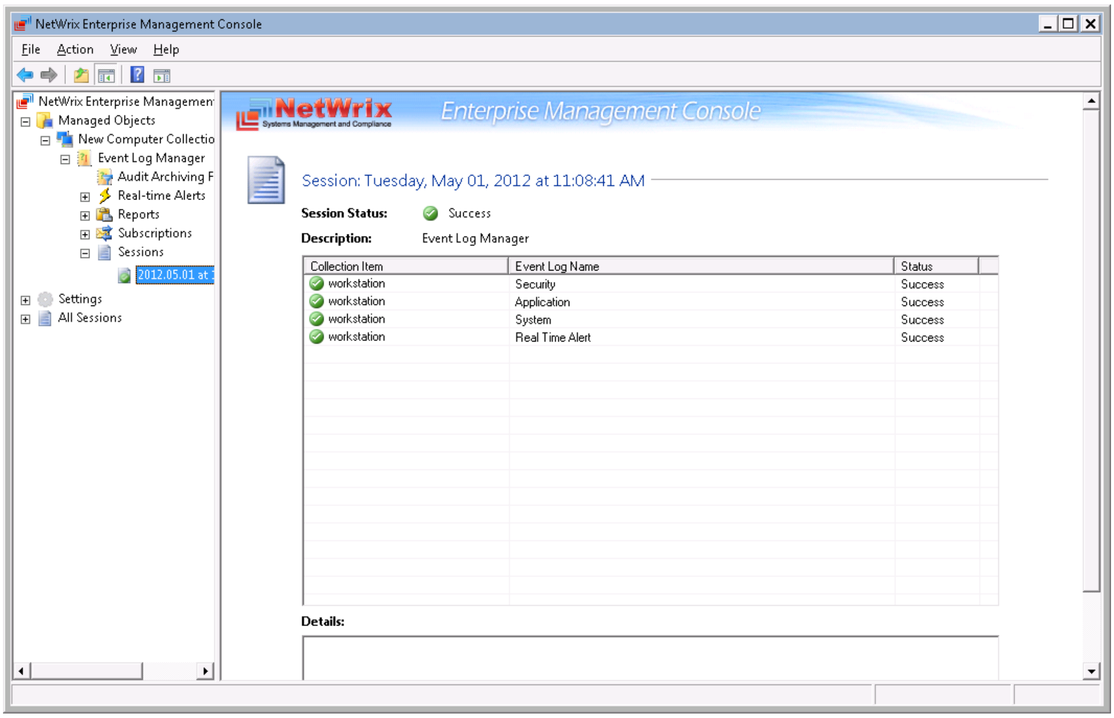
Field	Description
Date time	Date and time when an event was logged.
Event Source	The name of the software that logs an event.
Event Category	The number of an event defined by Event Source.
Event Type	Type of a logged event.

Event ID	The unique identifier of an event.
Event Log Name	The name of the Event log containing an event.
User	An account under which an event was generated.
Computer	The name of the computer where an event was generated.
Description	Detailed information on an event.
Event Parameters	Event-specific information from the EventData field of an event. This information can be viewed in Windows Event Viewer. **NOTE**: If an alert contains the **%String1%** … value under Event Parameters, this event has no information in the Event Data field.

10.2. Sessions

Each events summary delivery is referred to as 'Session' that shows data collection details. To view sessions for your Managed Object, expand the **Managed Objects** → **<your_managed_object>** → **Event Log Manager** → **Sessions** node and select a session. Session details will be displayed in the right pane:

Figure 63: Session Details Page



Session: Tuesday, May 01, 2012 at 11:08:41 AM

Session Status: Success

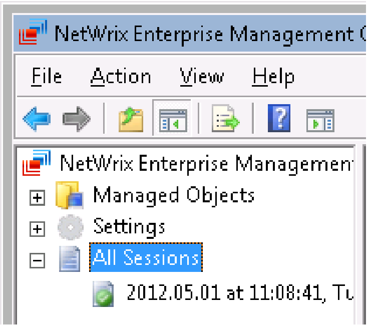
Description: Event Log Manager

Collection Item	Event Log Name	Status
workstation	Security	Success
workstation	Application	Success
workstation	System	Success
workstation	Real Time Alert	Success

Details:

You can also view sessions under the **All Sessions** node (all sessions for all installed NetWrix products are displayed here):

Figure 64: All Sessions Node


NetWrix Enterprise Management C
File Action View Help
NetWrix Enterprise Managemen
Managed Objects
Settings
All Sessions
2012.05.01 at 11:08:41, Tu

You can configure the number of sessions available for review in NetWrix Enterprise Management Console by specifying the date range for sessions to be displayed. For detailed instructions on how to do this, refer to Section 7.3 Configuring Audit Archive Settings.

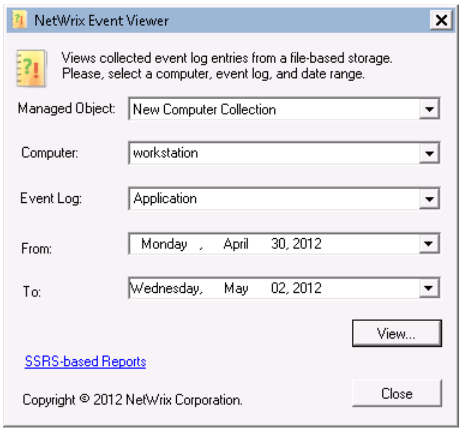
10.3. Viewing Audit Data in NetWrix Event Viewer

NetWrix Event Viewer allows viewing all data from the Audit Archive. You can view events collected within a specific period, from a specific computer or log. To view events, perform the following procedure:

Procedure 19. To view events in NetWrix Event Viewer

1. Navigate to **Start** → **All Programs** → **NetWrix** → **Event Log Manager** → **Advanced Tools** → **Viewer**. To do this, expand the **Managed Objects** → **<your_managed_object>** node and click the **Event Log Manager** node. In the right pane, click the **View** button under **Event Viewer**. NetWrix Event Viewer will be launched:

Figure 65: NetWrix Event Viewer



NetWrix Event Viewer

Views collected event log entries from a file-based storage.
Please, select a computer, event log, and date range.

Managed Object: New Computer Collection

Computer: workstation

Event Log: Application

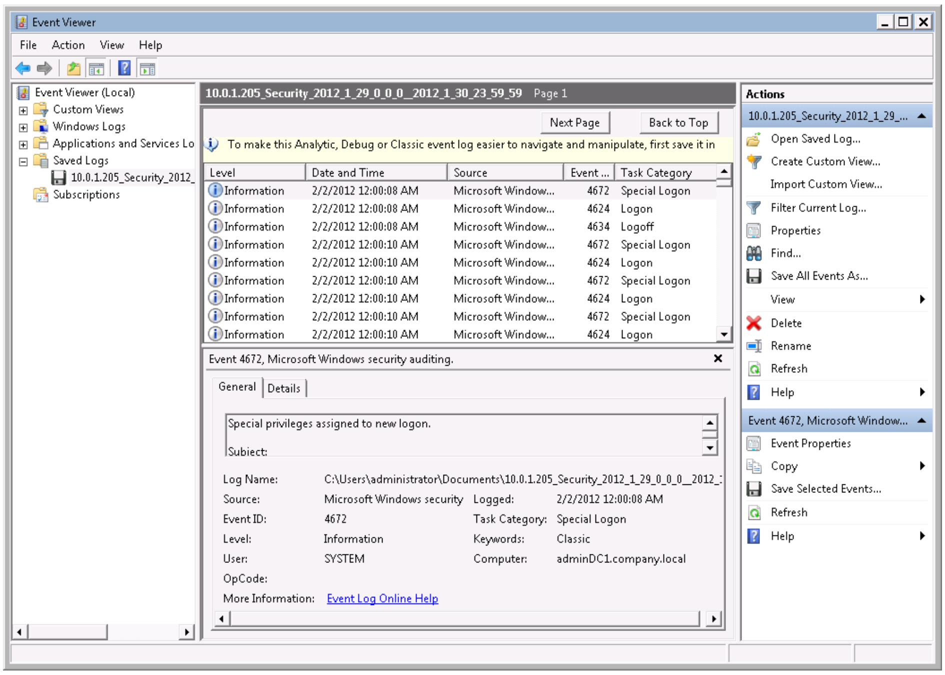
From: Monday , April 30, 2012

To: Wednesday, May 02, 2012

Copyright © 2012 NetWrix Corporation.

2. Set the parameters for selecting events from the Audit Archive and click the **View** button. Specify a folder where events must be uploaded.
3. The selected events will be written to an *.evt file. You can check them in the Windows Event Viewer.

Figure 66: Selected Events in Windows Event Viewer



To make this Analytic, Debug or Classic event log easier to navigate and manipulate, first save it in

Level	Date and Time	Source	Event ...	Task Category
Information	2/2/2012 12:00:08 AM	Microsoft Window...	4672	Special Logon
Information	2/2/2012 12:00:08 AM	Microsoft Window...	4624	Logon
Information	2/2/2012 12:00:08 AM	Microsoft Window...	4634	Logoff
Information	2/2/2012 12:00:10 AM	Microsoft Window...	4672	Special Logon
Information	2/2/2012 12:00:10 AM	Microsoft Window...	4624	Logon
Information	2/2/2012 12:00:10 AM	Microsoft Window...	4672	Special Logon
Information	2/2/2012 12:00:10 AM	Microsoft Window...	4624	Logon
Information	2/2/2012 12:00:10 AM	Microsoft Window...	4672	Special Logon
Information	2/2/2012 12:00:10 AM	Microsoft Window...	4624	Logon

Event 4672, Microsoft Windows security auditing.

Special privileges assigned to new logon.

Subject:

Log Name:	C:\Users\administrator\Documents\10.0.1.205_Security_2012_1_29_0_0_0__2012_:		
Source:	Microsoft Windows security	Logged:	2/2/2012 12:00:08 AM
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Classic
User:	SYSTEM	Computer:	adminDC1.company.local
OpCode:			
More Information:	Event Log Online Help		

11. Reports

In NetWrix Event Log Manager the following two report types are available:

- Events Summary
- SSRS-based Reports

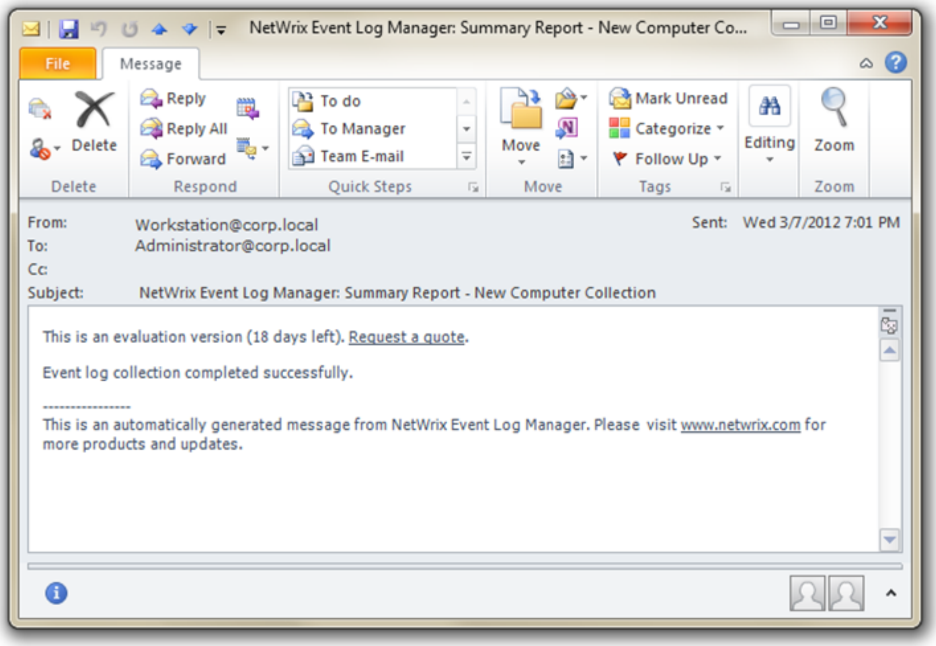
This chapter contains detailed instructions on how to use these reports, and provides report samples.

11.1. Events Summary

An events summary contains information on data collection errors that occurred since the last events summary delivery. By default, events summaries are delivered by email to the specified recipients every 24 hours.

If there were no errors, you will receive the following email:

Figure 67: Events Summary



From: Workstation@corp.local
To: Administrator@corp.local
Cc:
Subject: NetWrix Event Log Manager: Summary Report - New Computer Collection
Sent: Wed 3/7/2012 7:01 PM

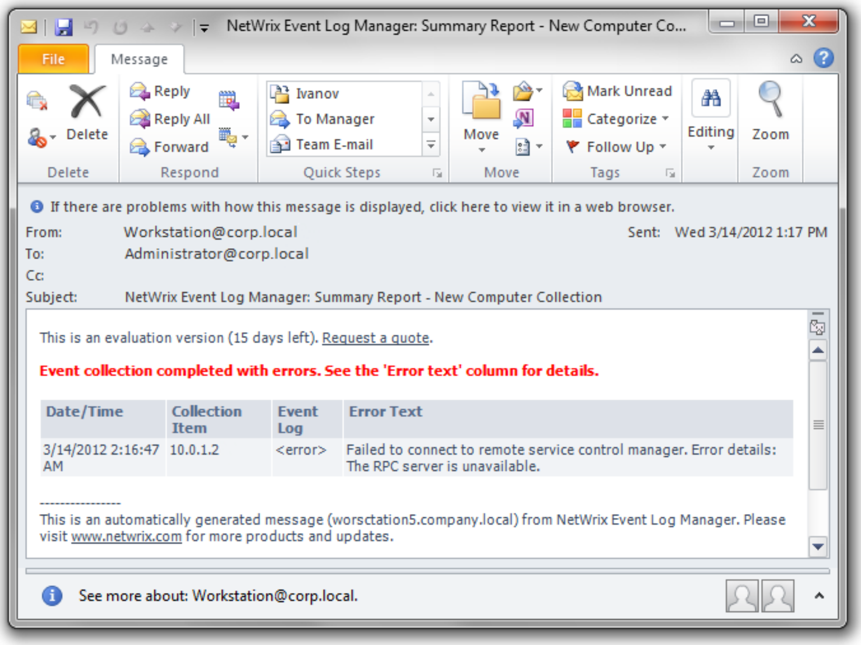
This is an evaluation version (18 days left). Request a quote.

Event log collection completed successfully.

This is an automatically generated message from NetWrix Event Log Manager. Please visit www.netwrix.com for more products and updates.

If an error is detected during data collection, the following email will be sent immediately to the specified recipients:

Figure 68: Email with the Error



If there are problems with how this message is displayed, click here to view it in a web browser.

From: Workstation@corp.local Sent: Wed 3/14/2012 1:17 PM
To: Administrator@corp.local
Cc:
Subject: NetWrix Event Log Manager: Summary Report - New Computer Collection

This is an evaluation version (15 days left). Request a quote.

Event collection completed with errors. See the 'Error text' column for details.

Date/Time	Collection Item	Event Log	Error Text
3/14/2012 2:16:47 AM	10.0.1.2	<error>	Failed to connect to remote service control manager. Error details: The RPC server is unavailable.

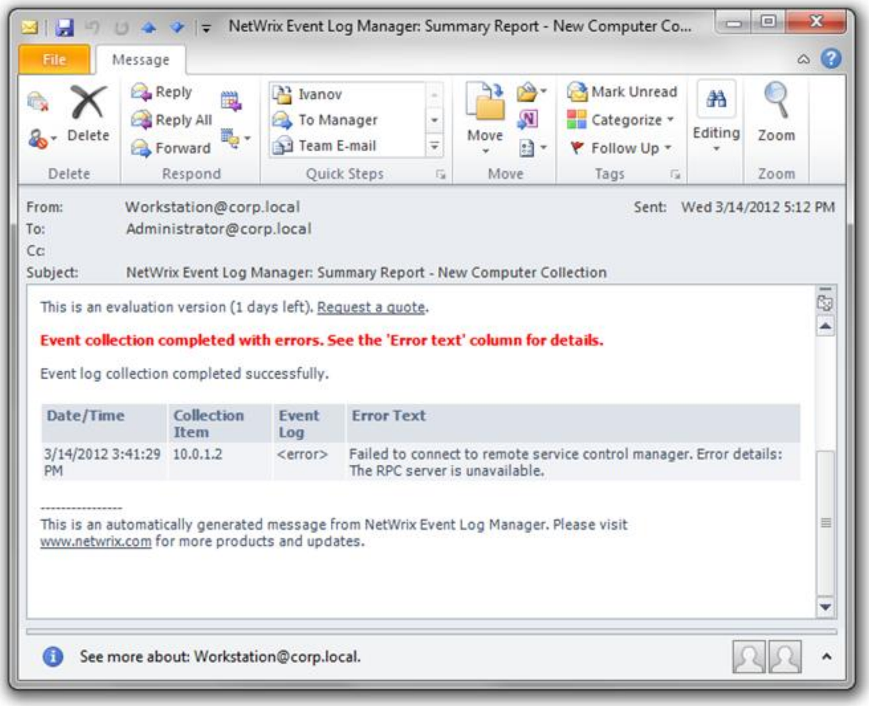
This is an automatically generated message (worsctation5.company.local) from NetWrix Event Log Manager. Please visit www.netwrix.com for more products and updates.

See more about: Workstation@corp.local.

Note: Even if this error is continually repeated, the notification is delivered once a day. You will receive a different error notification only if a new type of error is detected.

If this error is not fixed until an events summary delivery, you will receive an events summary with the error description like in the example below:

Figure 69: Events Summary with the Error



From: Workstation@corp.local Sent: Wed 3/14/2012 5:12 PM
To: Administrator@corp.local
Cc:
Subject: NetWrix Event Log Manager: Summary Report - New Computer Collection

This is an evaluation version (1 days left). Request a quote.

Event collection completed with errors. See the 'Error text' column for details.

Event log collection completed successfully.

Date/Time	Collection Item	Event Log	Error Text
3/14/2012 3:41:29 PM	10.0.1.2	<error>	Failed to connect to remote service control manager. Error details: The RPC server is unavailable.

This is an automatically generated message from NetWrix Event Log Manager. Please visit www.netwrix.com for more products and updates.

See more about: Workstation@corp.local.

11.2. SSRS-based Reports

The Event Log Manager functionality allows generating reports based on Microsoft SQL Server Reporting Services.

The product provides a wide variety of predefined report templates. Using these templates, you can generate reports covering all activities on the monitored computers and reports for regulatory compliances.

> **Note:** NetWrix Event Log Manager provides a comprehensive set of report templates that most probably meets your requirements. However, if your situation requires the use of additional report types, you can order custom report templates from NetWrix.

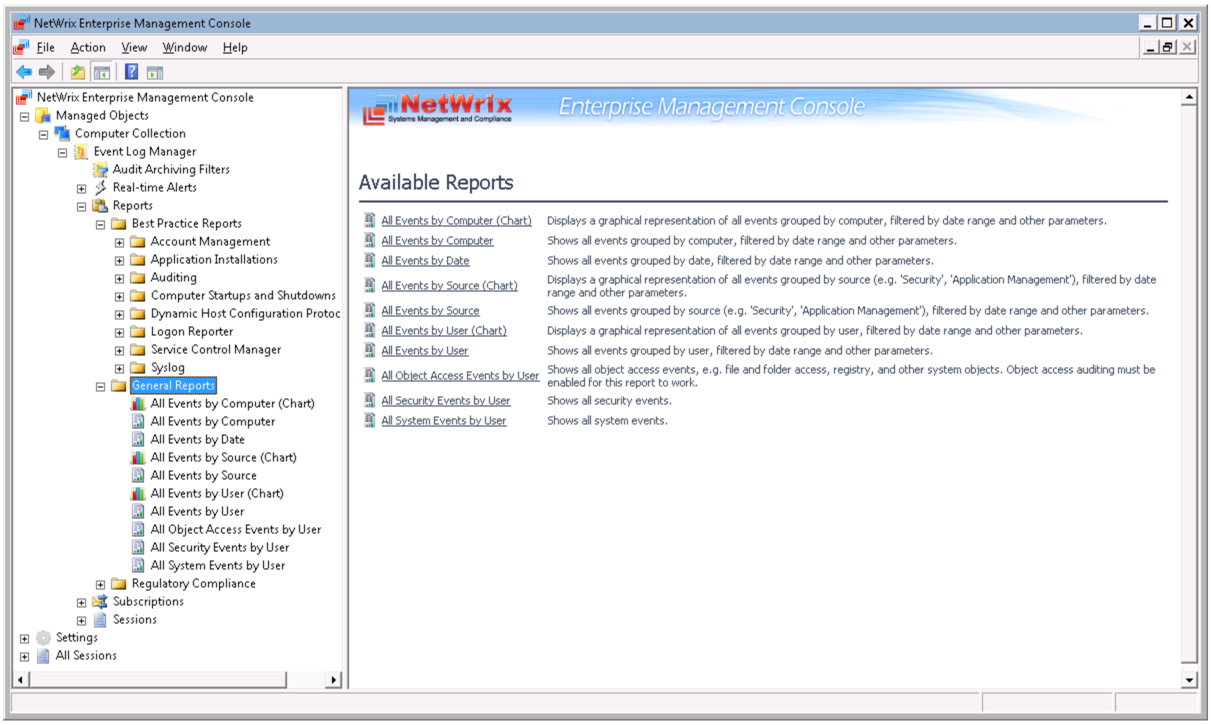
To access the reports, in NetWrix Enterprise Management Console navigate to **Managed Object → <your_managed_object> → Event Log Manager → Reports**.

Three groups of reports are available:

- Best Practice Reports
- General Reports
- Regulatory Compliance

For a full list of available reports in each category, expand the corresponding node:

Figure 70: Report Templates List


NetWrix Enterprise Management Console
File
Action
View
Window
Help
NetWrix
Systems Management and Compliance
Enterprise Management Console

- NetWrix Enterprise Management Console
  - Managed Objects
    - Computer Collection
      - Event Log Manager
        - Audit Archiving Filters
        - Real-time Alerts
        - Reports
          - Best Practice Reports
            - Account Management
            - Application Installations
            - Auditing
            - Computer Startups and Shutdowns
            - Dynamic Host Configuration Protoc
            - Logon Reporter
            - Service Control Manager
            - Syslog
          - General Reports
            - All Events by Computer (Chart)
            - All Events by Computer
            - All Events by Date
            - All Events by Source (Chart)
            - All Events by Source
            - All Events by User (Chart)
            - All Events by User
            - All Object Access Events by User
            - All Security Events by User
            - All System Events by User
          - Regulatory Compliance
        - Subscriptions
        - Sessions
  - Settings
  - All Sessions

Available Reports

All Events by Computer (Chart)	Displays a graphical representation of all events grouped by computer, filtered by date range and other parameters.
All Events by Computer	Shows all events grouped by computer, filtered by date range and other parameters.
All Events by Date	Shows all events grouped by date, filtered by date range and other parameters.
All Events by Source (Chart)	Displays a graphical representation of all events grouped by source (e.g. 'Security', 'Application Management'), filtered by date range and other parameters.
All Events by Source	Shows all events grouped by source (e.g. 'Security', 'Application Management'), filtered by date range and other parameters.
All Events by User (Chart)	Displays a graphical representation of all events grouped by user, filtered by date range and other parameters.
All Events by User	Shows all events grouped by user, filtered by date range and other parameters.
All Object Access Events by User	Shows all object access events, e.g. file and folder access, registry, and other system objects. Object access auditing must be enabled for this report to work.
All Security Events by User	Shows all security events.
All System Events by User	Shows all system events.

To collect events required for generating a specific report, you must select the filter whose name coincides with the report's name. To do this, in NetWrix Enterprise Management Console, navigate to **Managed Object → <your_managed_object> → Event Log Manager → Audit Archiving Filters** and select the required check boxes.

Reports can be viewed using one of the following:

- Viewing Reports in the Enterprise Management Console
- Viewing Reports in a Web Browser

- Viewing Reports by Configuring Subscriptions

Refer to the sections below for detailed instructions on these options.

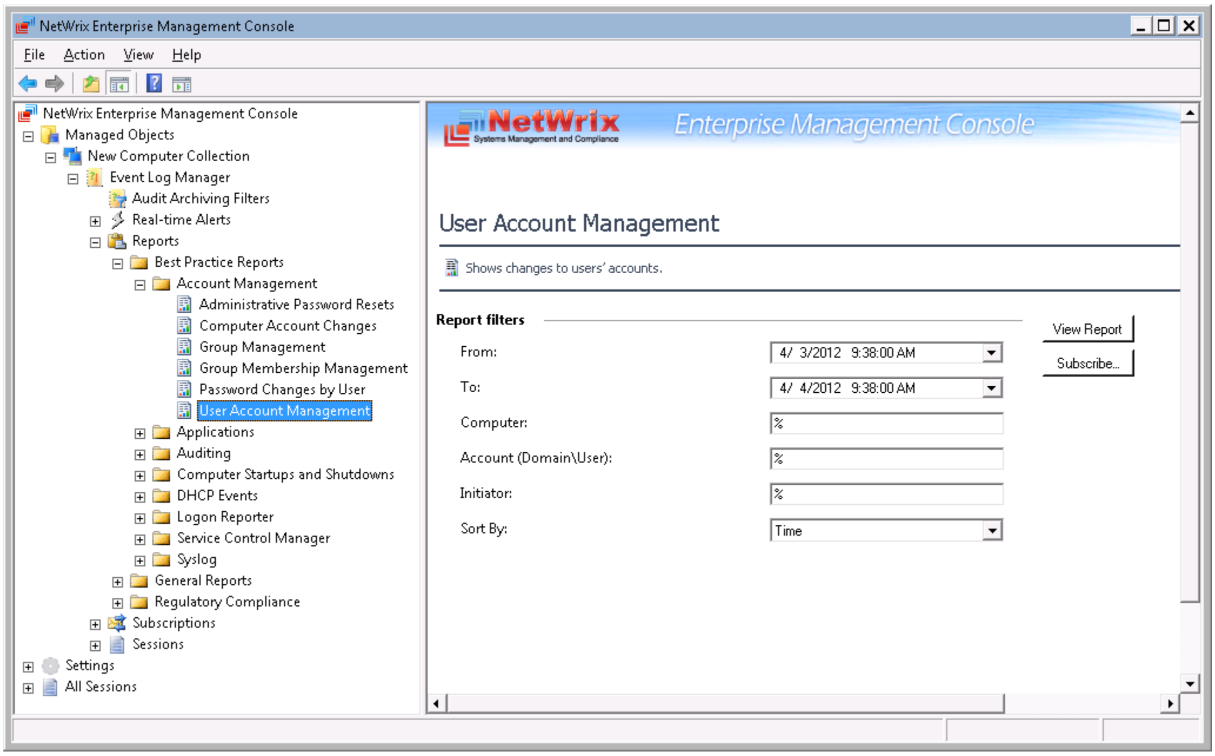
11.2.1. Viewing Reports in the Enterprise Management Console

To view a report in NetWrix Enterprise Management Console, perform the following procedure:

Procedure 20. To view a report in NetWrix Enterprise Management Console

1. Navigate to **Managed Objects → <your_managed_object> → Event Log Manager → Reports → <report_type>** and select the report you want to view. The following page will be displayed (details may vary slightly depending on the selected report):

Figure 71: Reports: User Account Management



User Account Management

Shows changes to users' accounts.

Report filters

From: 4/ 3/2012 9:38:00 AM

To: 4/ 4/2012 9:38:00 AM

Computer: %

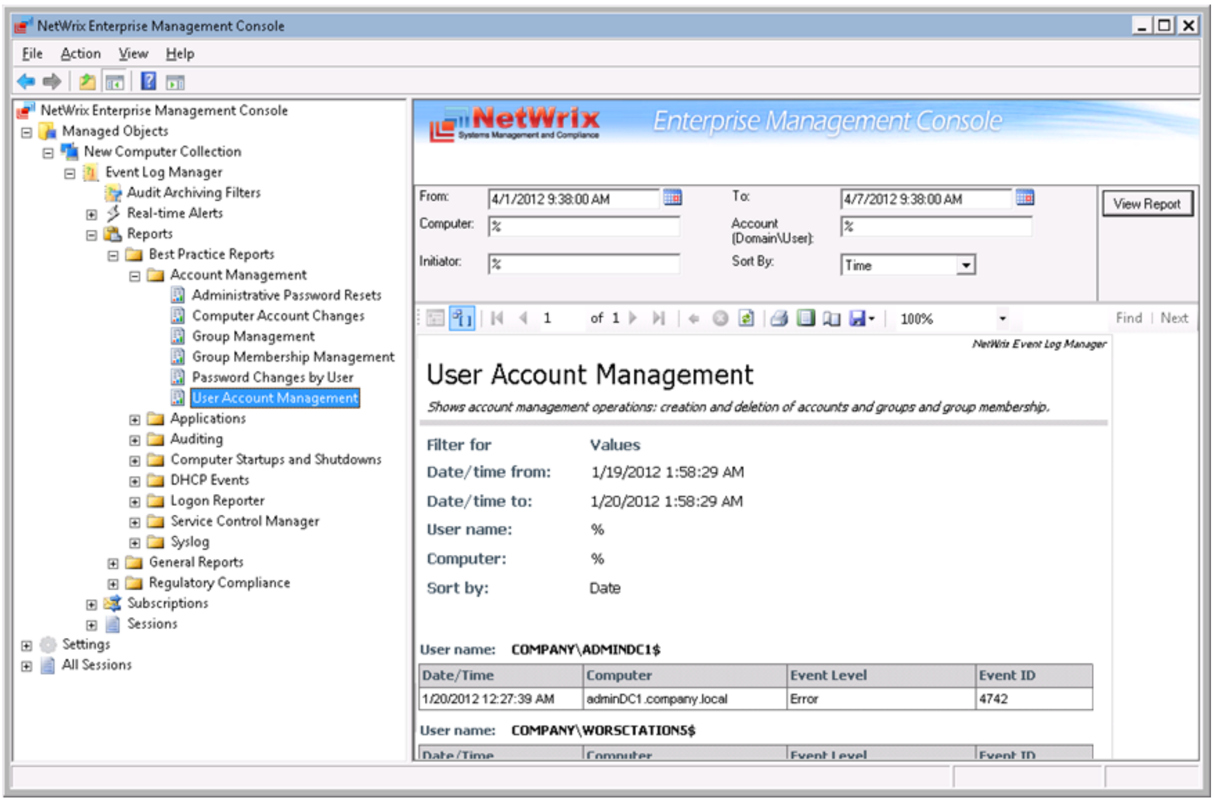
Account (Domain\User): %

Initiator: %

Sort By: Time

2. Specify the report filters and click the **View Report** button to generate the report:

Figure 72: User Account Management Report



From: 4/1/2012 9:38:00 AM
To: 4/7/2012 9:38:00 AM
Computer: %
Account (Domain\User): %
Initiator: %
Sort By: Time

User Account Management

Shows account management operations: creation and deletion of accounts and groups and group membership.

Filter for	Values
Date/time from:	1/19/2012 1:58:29 AM
Date/time to:	1/20/2012 1:58:29 AM
User name:	%
Computer:	%
Sort by:	Date

User name: COMPANY\ADMINDC1$

Date/Time	Computer	Event Level	Event ID
1/20/2012 12:27:39 AM	adminDC1.company.local	Error	4742

User name: COMPANY\WORSCTATIONS$

Date/Time	Computer	Event Level	Event ID

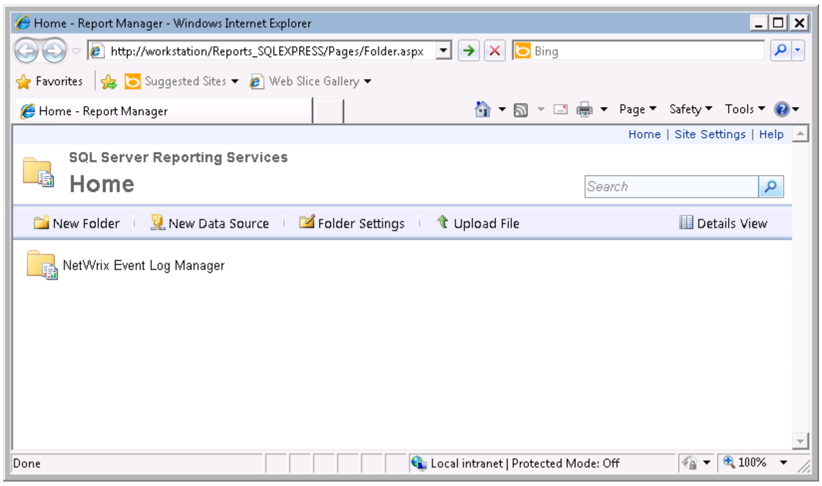
11.2.2. Viewing Reports in a Web Browser

To view a report in a web browser, perform the following procedure:

Procedure 21. To view a report in a web browser

1. Open your web browser.
2. Specify the SQL Server Report Manager URL (to find the Report Manager URL, in NetWrix Enterprise Management Console navigate to **Settings** → **Reports**. You will find the Report Manager URL under **SQL Reporting Services** in the right pane). Press **Enter.** The following page will be displayed:

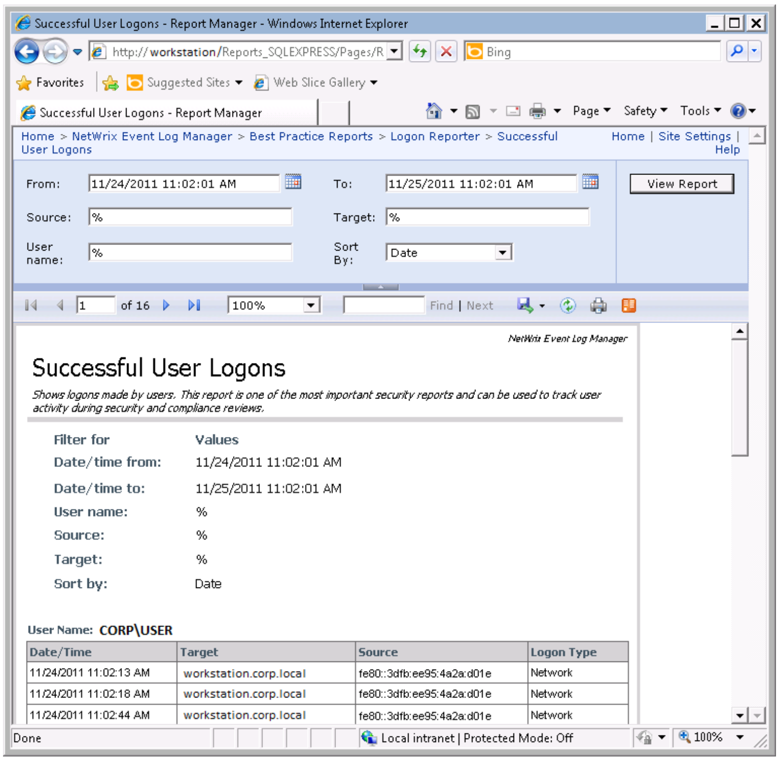
Figure 73: SQL Server Reporting Services Home Page


Home - Report Manager - Windows Internet Explorer
Bing
Favorites
Suggested Sites
Web Slice Gallery
Home - Report Manager
Page
Safety
Tools
Home | Site Settings | Help
SQL Server Reporting Services
Home
Search
New Folder
New Data Source
Folder Settings
Upload File
Details View
NetWrix Event Log Manager
Done
Local intranet | Protected Mode: Off
100%

http://workstation/Reports_SQLEXPRESS/Pages/Folder.aspx

3. Click **NetWrix Event Log Manager**. Select the report you want to generate. On the page that opens, a report showing events for the last 24 hours will be displayed:

Figure 74: Successful User Logons Report


Successful User Logons - Report Manager - Windows Internet Explorer
http://workstation/Reports_SQLEXPRESS/Pages/R
Bing
Favorites
Suggested Sites
Web Slice Gallery
Successful User Logons - Report Manager
Page
Safety
Tools
Home > NetWrix Event Log Manager > Best Practice Reports > Logon Reporter > Successful User Logons
Home | Site Settings | Help
View Report
1 of 16
100%
Find | Next
NetWrix Event Log Manager
Done
Local intranet | Protected Mode: Off
100%

From: 11/24/2011 11:02:01 AM To: 11/25/2011 11:02:01 AM

Source: % Target: %

User name: % Sort By: Date

Successful User Logons

Shows logons made by users. This report is one of the most important security reports and can be used to track user activity during security and compliance reviews.

Filter for	Values
Date/time from:	11/24/2011 11:02:01 AM
Date/time to:	11/25/2011 11:02:01 AM
User name:	%
Source:	%
Target:	%
Sort by:	Date

User Name: **CORP\USER**

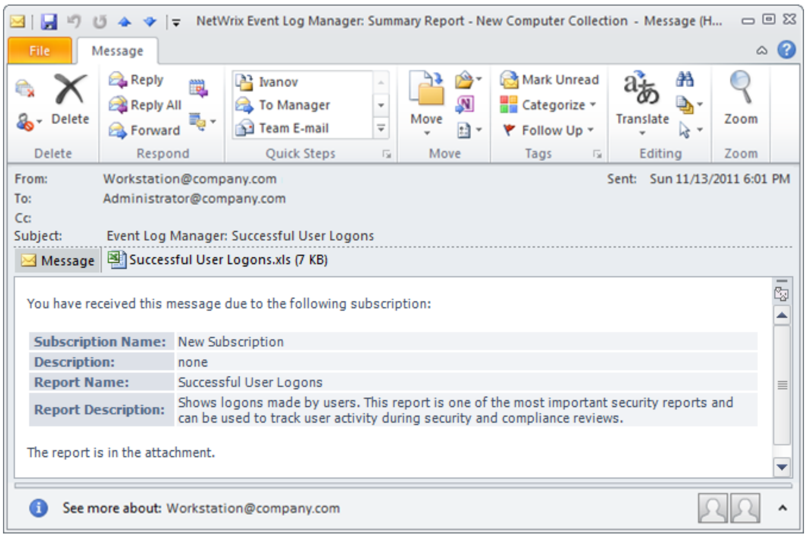
Date/Time	Target	Source	Logon Type
11/24/2011 11:02:13 AM	workstation.corp.local	fe80::3dfb:ee95:4a2a:d01e	Network
11/24/2011 11:02:18 AM	workstation.corp.local	fe80::3dfb:ee95:4a2a:d01e	Network
11/24/2011 11:02:44 AM	workstation.corp.local	fe80::3dfb:ee95:4a2a:d01e	Network

Also, on this page you can specify report filters to generate a report with required settings.

11.2.3. Viewing Reports by Configuring Subscriptions

For information on how to configure a subscription, refer to Chapter 6 Configuring Subscriptions to Reports. If a subscription is configured, reports will be delivered on schedule by email to the specified recipients. A file with the report in a specified format is attached to the email:

Figure 75: Successful User Logons Email



From: Workstation@company.com Sent: Sun 11/13/2011 6:01 PM
To: Administrator@company.com
Cc:
Subject: Event Log Manager: Successful User Logons

Successful User Logons.xls (7 KB)

You have received this message due to the following subscription:

Subscription Name:	New Subscription
Description:	none
Report Name:	Successful User Logons
Report Description:	Shows logons made by users. This report is one of the most important security reports and can be used to track user activity during security and compliance reviews.

The report is in the attachment.

A APPENDIX: SUPPORTING DATA

A.1 Event Log Manager Registry Keys

The table below contains the description of the basic NetWrix Event Log Manager registry keys that you may need to configure while using the product:

Table 11: NetWrix Event Log Manager Registry Keys

Registry Key	Type	Description/Value
HKEY_LOCAL_MACHINE\SOFTWARE\NetWrix\Event Log Manager\<Managed Object Name>\Database Settings		
Ar_enabled	REG_DWORD	Defines the Reports feature status: 0 - disabled 1 - enabled
ConnectionTimeout	REG_DWORD	Defines SQL database connection timeout (in seconds).
HKEY_LOCAL_MACHINE\SOFTWARE\NetWrix\Event Log Manager\<Managed Object Name>\ElmDbOptions		
BatchSize	REG_DWORD	Defines the number of entries processed in a batch (must be more than 1000).
BatchTimeOut	REG_DWORD	Defines batch writing timeout (in seconds).
DeadLockErrorCount	REG_DWORD	Defines the number of write attempts to a SQL database.
HKEY_LOCAL_MACHINE\SOFTWARE\NetWrix\Event Log Manager\<Managed Object Name>		
CleanAutoBackupLogs	REG_DWORD	Defines Backup Log deletion delay (in hours).
ProcessBackupLogs	REG_DWORD	Defines Backup Log processing status: 0 - disabled 1 - enabled
WriteAgentsToApplicationLog	REG_DWORD	Defines the capability of writing events of the Event Log Manager Agent to the Application Log of a monitored machine: 0 - disabled 1 - enabled
WriteToApplicationLog	REG_DWORD	Defines the capability of writing events produced by NetWrix Event Log Manager operation to the Application Log of the machine where the product is installed: 0 - disabled 1 - enabled

A.2 Related Documentation

The table below lists all documents available to support NetWrix Event Log Manager:

Table 12: Product Documentation

Document Name	Overview
NetWrix Event Log Manager Administrator’s Guide	The current document.
NetWrix Event Log Manager Installation and Configuration Guide	Provides detailed instructions on how to install and configure NetWrix Event Log Manager.

NetWrix Event Log Manager Quick-Start Guide (Enterprise Edition)	Provides an overview of the product's functionality, and instructions on how to install, configure and start using NetWrix Event Log Manager (Enterprise Edition).
NetWrix Event Log Manager Quick-Start Guide (Freeware Edition)	Provides an overview of the product's functionality, and instructions on how to install, configure and start using NetWrix Event Log Manager (Freeware Edition).
NetWrix Event Log Manager User Guide	Provides information on different NetWrix Event Log Manager reporting capabilities, lists all available report types and report formats, and explains how these reports can be viewed and interpreted.
NetWrix Event Log Manager Release Notes	The document provides a list of known issues that customer may experience while using the release version 4.0.