# NetWrix Event Log Manager

## Quick-Start Guide

## for the Freeware Edition

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 is intended for first-time users of NetWrix Event Log Manager Freeware Edition. It contains an overview of the product functionality, and instructions on how to install, configure and start using the product.

This guide can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided.

After reading this guide you will be able to:

- Install and configure NetWrix Event Log Manager;
- Run data collection;
- Receive an events summary and a real-time alert.

**Note:** This guide only covers the product's Freeware Edition. For information on the full product functionality available in NetWrix Event Log Manager Enterprise Edition, refer to NetWrix Event Log Manager Administrator's Guide.

## 1.2. How This Guide is Organized

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

- Chapter 1 Introduction: the current chapter. It explains the purpose of this document, defines its audience and explains its structure.
- Chapter 2 Product Overview: contains an overview of the product, lists its main features and explains its architecture and workflow. It also contains information on licensing.
- Chapter 3 Installing NetWrix Event Log Manager: lists all hardware and software requirements for the installation of NetWrix Event Log Manager Freeware Edition. It also provides information on requirements to the monitored environment and instructions on how to install the product.
- Chapter 4 Configuring Target : provides instructions on how to configure the computers that will be monitored.
- Chapter 5 Configuring NetWrix Event Log Manager Freeware Edition: explains how to configure the product's settings.
- Chapter 6 Monitoring Your : explains how to manually generate an events summary and contains notification examples.
- Appendix: Related Documentation: contains 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 the required events. NetWrix Event Log Manager Freeware Edition provides the following functionality:

- Consolidation of all event log 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.
- Detection of critical events and sending of email alerts.

## 2.2. Product Workflow

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

1. The administrator specifies the computers to be monitored.
2. The administrator sets parameters for automated data collection, and defines types of events that must trigger alerts and need be written to the Audit Archive (local file storage).
3. NetWrix Event Log Manager collects all new event log entries and archives them in the Audit Archive. These 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 events summary recipients.
5. An event summary is emailed to the specified recipients every 24 hours.

## 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 compliance | 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 | No | Yes |

| | | |
|---|---|---|
| computer collections, each with its own individual settings | | |
| 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 and settings 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. INSTALLING NETWRIX EVENT LOG MANAGER

## 3.1. Installation Prerequisites

NetWrix Event Log Manager can be installed on any computer in the domain that your target computers belong to, or in a trusted domain, but it is not recommended to install it on a domain controller.

### 3.1.1. Hardware Requirements

Before installing NetWrix Event Log Manager Freeware Edition, make sure that your system meets the following hardware requirements:

*Table 2: NetWrix Event Log Manager Hardware Requirements*

| Component | Minimum | Recommended |
|---|---|---|
| Processor | Intel or AMD 32 bit, 2GHz | Intel or AMD 64 bit, 3GHz |
| Memory | 512MB RAM | 2GB RAM |
| Disk* | 50MB physical disk space for the installation | 20GB free space |

* *Approximately 500 bytes of disk space are required per each event.*

### 3.1.2. Software Requirements

Before installing NetWrix Event Log Manager Freeware Edition, make sure that your system meets the following software requirements:

*Table 3: NetWrix Event Log Manager Software Requirements*

| Component | Requirement |
|---|---|
| Operating System | Windows XP SP3 or later |
| Framework | .NET Framework 2.0, 3.0 or 3.5 |

### 3.1.3. Target Computers Requirements

The following requirements apply to Event Log Manager Freeware Edition target computers:

*Table 4: Target Computers Requirements*

| Component | Requirement |
|---|---|
| Operating System | Windows 2000 or later |
| Services | Make sure that the Remote Registry service is started. |

## 3.2. Installing NetWrix Event Log Manager

To install NetWrix Event Log Manager Freeware Edition, perform the following procedure:

### Procedure 1. To install NetWrix Event Log Manager

1. Download NetWrix Event Log Manager Freeware Edition.
2. Run the setup package called elmfree_setup.msi.
3. Follow the instructions of the installation wizard.
4. When prompted, accept the license agreement and specify the installation folder.
5. On the last step, click **Finish** to complete the installation.

The NetWrix Event Log Manager (Freeware Edition) shortcut will be added to your **Start** menu.

**Note:** NetWrix Event Log Manager Freeware Edition runs as a service, therefore it is not necessary to keep the program open once it has been configured.

# 4. Configuring Target Computers

For NetWrix Event Log Manager to work properly, the Remote Registry service must be enabled on the target computers.

> **Note:** This is only required if you are *not* going to use the **Network Traffic Compression** option.

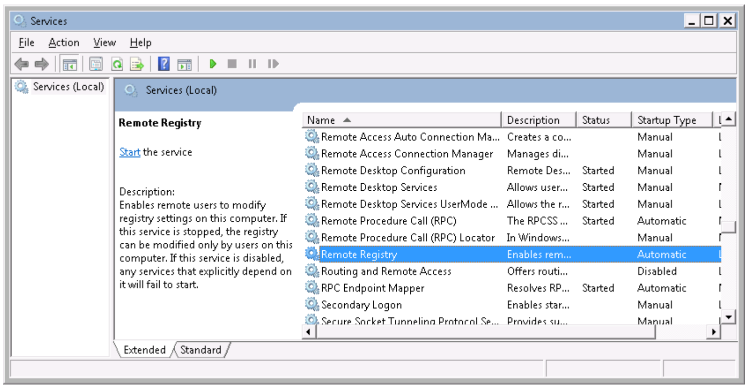
Verify that the service has been started on the machines that you want to monitor for events, otherwise run the service.

To enable the service, perform the following procedure:

## Procedure 2. To enable the Remote Registry service

1. Navigate to **Start** → **Run.** Type `Services.msc` and click **OK.** In the **Services** dialog proceed to the **Remote Registry** service:

*Figure 1: The Services Dialog*



**Remote Registry**

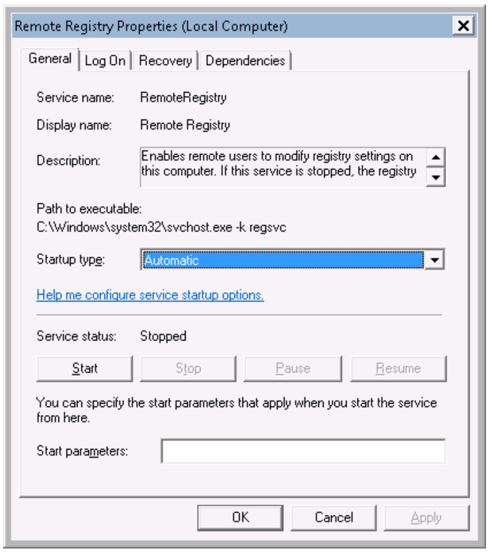
Start the service

Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

| Name | Description | Status | Startup Type |
|---|---|---|---|
| Remote Access Auto Connection Ma... | Creates a co... |  | Manual |
| Remote Access Connection Manager | Manages di... |  | Manual |
| Remote Desktop Configuration | Remote Des... | Started | Manual |
| Remote Desktop Services | Allows user... | Started | Manual |
| Remote Desktop Services UserMode ... | Allows the r... | Started | Manual |
| Remote Procedure Call (RPC) | The RPCSS ... | Started | Automatic |
| Remote Procedure Call (RPC) Locator | In Windows... |  | Manual |
| Remote Registry | Enables rem... |  | Automatic |
| Routing and Remote Access | Offers routi... |  | Disabled |
| RPC Endpoint Mapper | Resolves RP... | Started | Automatic |
| Secondary Logon | Enables star... |  | Manual |
| Secure Socket Tunneling Protocol Se... | Provides su... |  | Manual |

2. Right-click the **Remote Registry** service and select **Properties.** In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to **Automatic** and click the **Start** button:

*Figure 2: The Remote Registry Properties Dialog*



Service name: RemoteRegistry

Display name: Remote Registry

Description: Enables remote users to modify registry settings on this computer. If this service is stopped, the registry

Path to executable:
C:\Windows\system32\svchost.exe -k regsvc

Startup type: Automatic

Help me configure service startup options.

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

3. Click **OK** to save the changes.
4. In the **Services** dialog, ensure that the **Remote Registry** status has changed to **Started.**

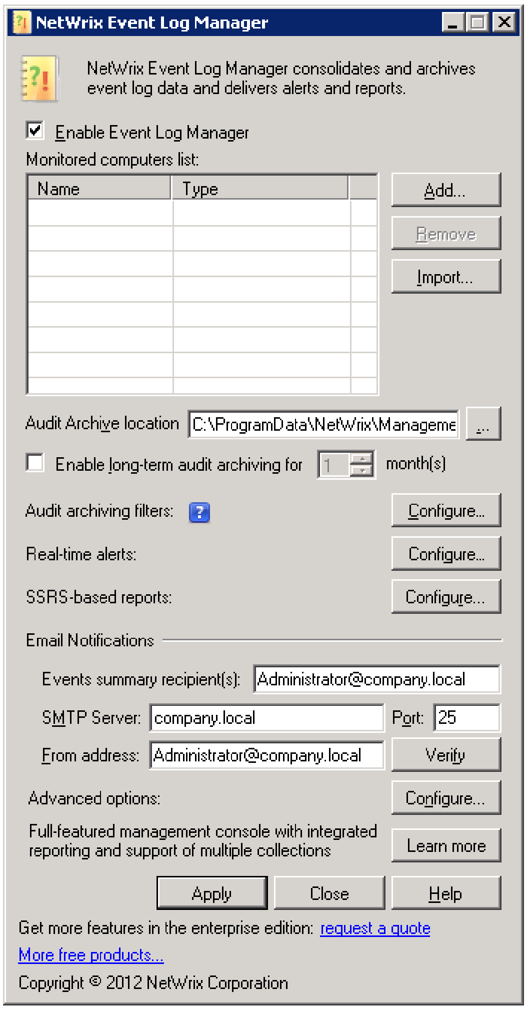
# 5. Configuring NetWrix Event Log Manager Freeware Edition

After you have installed NetWrix Event Log Manager and configured your target computers, you must configure the product:

## Procedure 3. To configure NetWrix Event Log Manager Freeware Edition

1. Navigate to **Start → All Programs → NetWrix Freeware → Event Log Manager → Event Log Manager (Freeware Edition)** to open the product's configuration dialog:

*Figure 3: The NetWrix Event Log Manager Configuration Dialog*



NetWrix Event Log Manager

NetWrix Event Log Manager consolidates and archives event log data and delivers alerts and reports.

☑ Enable Event Log Manager

Monitored computers list:

| Name | Type |
|---|---|

Audit Archive location: C:\ProgramData\NetWrix\Manageme

☐ Enable long-term audit archiving for 1 month(s)

Audit archiving filters:

Real-time alerts:

SSRS-based reports:

Email Notifications

Events summary recipient(s): Administrator@company.local

SMTP Server: company.local Port: 25

From address: Administrator@company.local

Advanced options:

Full-featured management console with integrated reporting and support of multiple collections

Get more features in the enterprise edition: request a quote

More free products...

Copyright © 2012 NetWrix Corporation

2. Specify the following settings and parameters:

**Note:** The table below describes configuration of the basic parameters required for the product evaluation purposes.

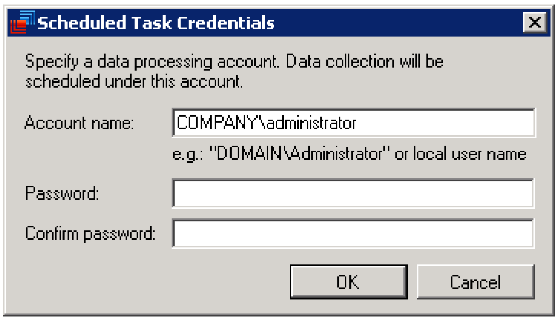
*Figure 4: NetWrix Event Log Manager Freeware Edition Settings*

| Parameter | Instruction |
|---|---|
| Enable Event Log Manager | Make sure this option is selected. |
| Monitored computers list | Click the **Add** button and enter an IP address or computer name. |

| | |
|---|---|
| | You can also remove computers you have specified previously from the list. |
| Real-time alerts | 1. Click the **Configure** button.<br>2. In the dialog that opens, click **Add**.<br>3. In the **Real-time Alerts Properties** dialog, make sure that the **Enable this alert** check box is selected, enter the alert name in the **Name** field (for example "NetWrix Event Log Agents") and click **Add** under **Event filters**.<br>4. In the **Event Filters** dialog, select the **Event Fields** tab.<br>5. In the **Event ID** field, specify the value by which all events will be filtered. You will receive real-time alerts on the events containing this value in ID.<br>6. Save the changes. |
| Events summary recipient(s) | Enter email addresses of events summary recipients, separated by commas. |
| SMTP server | Enter your SMTP server name. |
| Port | Enter your SMTP server port number. |
| From address | Enter the email that will appear in the "From" field in events summaries and alerts.<br>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. |
| The following settings are available for **Advanced Options** by clicking the **Configure** button | |
| Enable network traffic compression | Make sure this option is selected. |
| Daily Events Summary delivery time | Specify time. Events summaries will be delivered daily at this time. |
| Use SMTP authentication | Select this check box if your mail server requires SMTP authentication. |
| User name | Enter the user name for SMTP authentication. |
| Password | Enter the password for SMTP authentication. |
| Confirm password | Enter the password for SMTP authentication. |
| Use Secure Sockets Layer encrypted connection (SSL) | Select this checkbox if your SMTP server requires SSL to be enabled. |
| Use Implicit SSL connection mode | Select this checkbox if implicit SSL mode is used, which means that SSL connection is established before any meaningful data is sent. |

3. Save your configuration by clicking the **Apply** button. The following dialog will be displayed:

*Figure 5: The Scheduled Task Credentials Dialog*



Scheduled Task Credentials

Specify a data processing account. Data collection will be scheduled under this account.

Account name: COMPANY\administrator

e.g.: "DOMAIN\Administrator" or local user name

Password:

Confirm password:

4. Enter the data processing account (<domain name>\<account name>) that will be used by NetWrix Event Log Manager Freeware Edition 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.

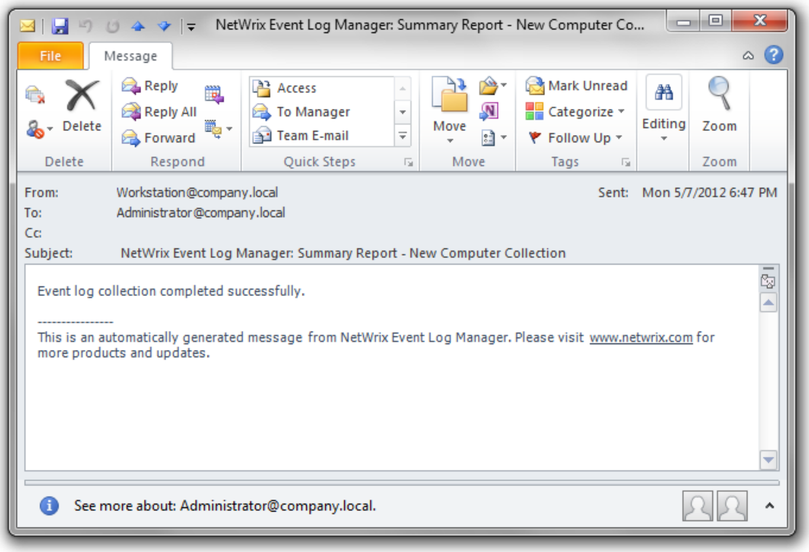
5. Click **OK** to save the changes**.**

# 6. Monitoring Your Computers for Events

When the product is configured, NetWrix Event Log Manager starts collecting events from computers according to the specified filters and stores them in the Audit Archive.

Events summary will be delivered daily at the time, specified in the **Daily Events Summary delivery time** setting:

*Figure 6: Events Summary*



From: Workstation@company.local
To: Administrator@company.local
Cc:
Subject: NetWrix Event Log Manager: Summary Report - New Computer Collection
Sent: Mon 5/7/2012 6:47 PM

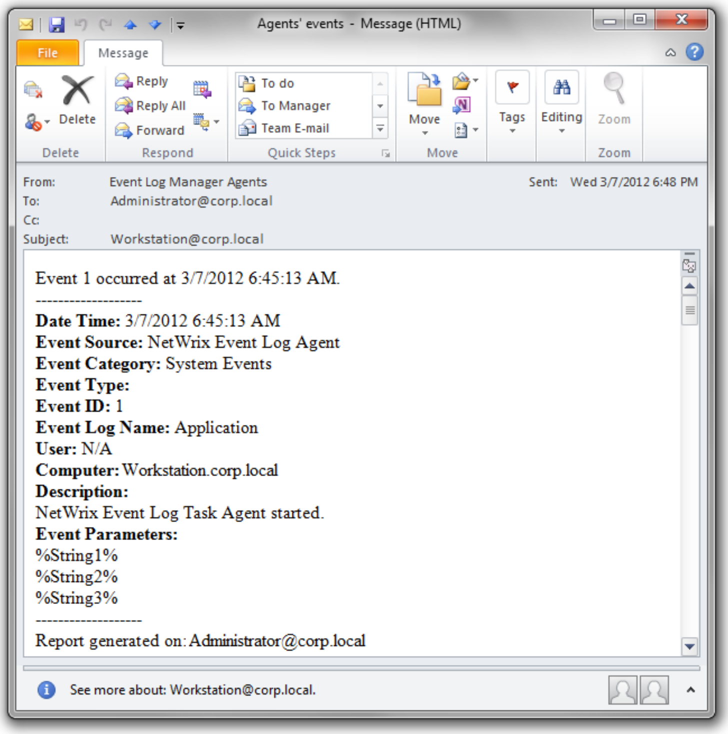
Event log collection completed successfully.

---------------

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

After the product detects the required events, it will send notifications to the event summary recipients. The following figure illustrates an alert for the NetWrix Event Log Manager Agents event:

*Figure 7: Example Real-Time Alert*



From: Event Log Manager Agents
To: Administrator@corp.local
Cc:
Subject: Workstation@corp.local
Sent: Wed 3/7/2012 6:48 PM

Event 1 occurred at 3/7/2012 6:45:13 AM.

-------------------

**Date Time:** 3/7/2012 6:45:13 AM
**Event Source:** NetWrix Event Log Agent
**Event Category:** System Events
**Event Type:**
**Event ID:** 1
**Event Log Name:** Application
**User:** N/A
**Computer:** Workstation.corp.local
**Description:**
NetWrix Event Log Task Agent started.
**Event Parameters:**
%String1%
%String2%
%String3%

-------------------

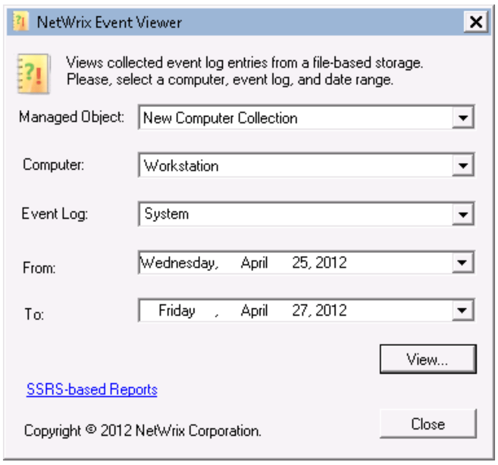
Report generated on: Administrator@corp.local

To view collected events, perform the following procedure:

## Procedure 4. To view collected events

1. Navigate to **Start → All programs → NetWrix → Event Log Manager → Advanced Tools → Viewer**. NetWrix Event Viewer will open:

*Figure 8: 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: System

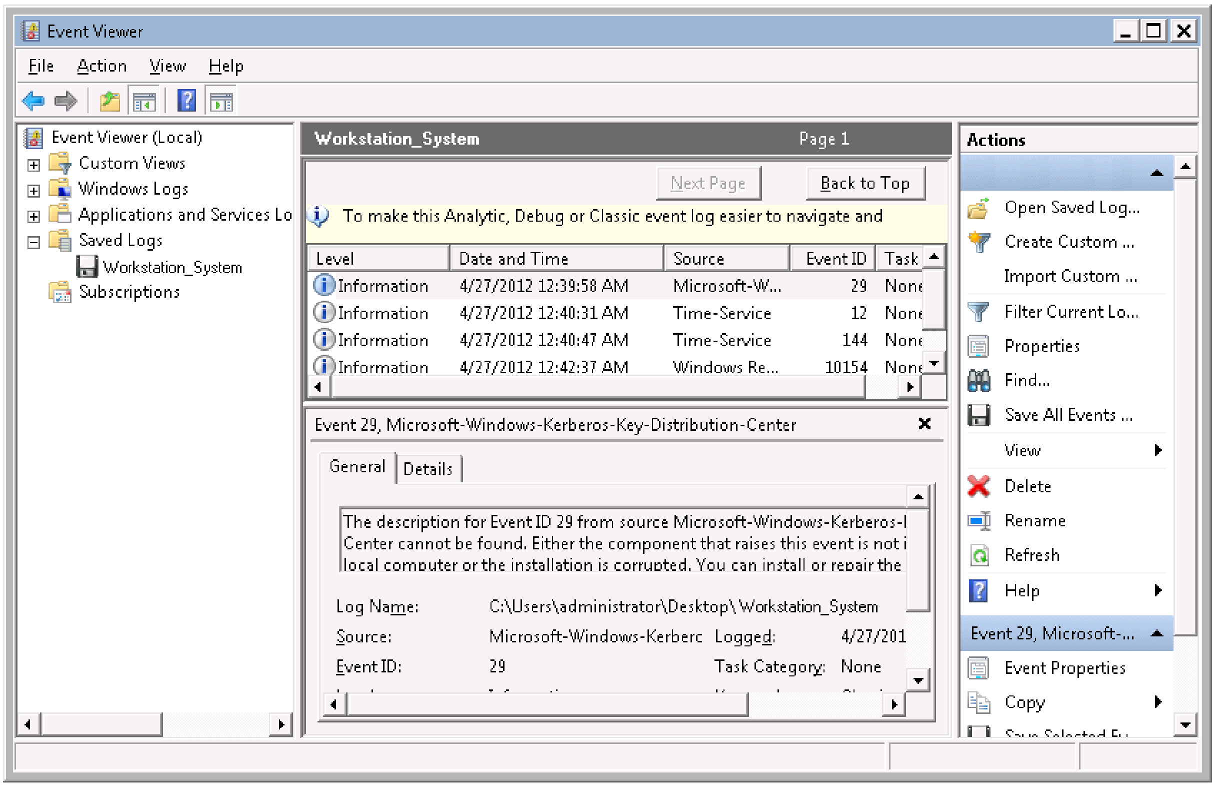
From: Wednesday, April 25, 2012

To: Friday , April 27, 2012

Copyright © 2012 NetWrix Corporation.

2. Select the Event Log you want to view, specify the date range for events to be displayed and click the **View** button.
3. Select the location to write events to and click **Save**. The selected events will be displayed in Windows Event Viewer:

*Figure 9: Event Viewer*



To make this Analytic, Debug or Classic event log easier to navigate and

| Level | Date and Time | Source | Event ID | Task |
|---|---|---|---|---|
| Information | 4/27/2012 12:39:58 AM | Microsoft-W... | 29 | None |
| Information | 4/27/2012 12:40:31 AM | Time-Service | 12 | None |
| Information | 4/27/2012 12:40:47 AM | Time-Service | 144 | None |
| Information | 4/27/2012 12:42:37 AM | Windows Re... | 10154 | None |

Event 29, Microsoft-Windows-Kerberos-Key-Distribution-Center

The description for Event ID 29 from source Microsoft-Windows-Kerberos-I
Center cannot be found. Either the component that raises this event is not i
local computer or the installation is corrupted. You can install or repair the

Log Name: C:\Users\administrator\Desktop\Workstation_System

Source: Microsoft-Windows-Kerberc Logged: 4/27/201

Event ID: 29 Task Category: None

# A APPENDIX: RELATED DOCUMENTATION

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

*Table 5: Product Documentation*

| Document Name | Overview |
|---|---|
| NetWrix Event Log Manager Quick-Start Guide (Freeware Edition) | The current document. |
| NetWrix Event Log Manager Administrator's Guide | Provides detailed instructions on how to configure and use NetWrix Event Log Manager. |
| NetWrix Event Log Manager Installation and Configuration Guide | Provides detailed instructions on how to install NetWrix Event Log Manager and configure monitored computers. |
| 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 User Guide | Provides information on different NetWrix Event Log Manager reporting capabilities and 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. |