NETWRIX EVENT LOG MANAGER

INSTALLATION AND CONFIGURATION 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 provides detailed instructions on how to install and set up NetWrix Event Log Manager, lists all product requirements and explains how to configure the target computers.

This guide can be used by system integrators and administrators.

For information on how to configure auditing and reporting settings, 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 Deployment Options provides information and recommendations on how to deploy the product.
- Chapter 3 Installation Prerequisites: lists all product requirements, as well as requirements to the target machines and supported Microsoft SQL Server versions.
- Chapter 4 Installing NetWrix Event Log Manager: contains instructions on how to install NetWrix Event Log Manager.
- Chapter 5 Configuring Target Computers: explains how to configure your target computers for auditing.
- Chapter 6 Upgrading from Previous Versions: contains instructions on how to upgrade NetWrix Event Log Manager.
- Chapter 7 Uninstalling NetWrix Event Log Manager: explains how to uninstall NetWrix Event Log Manager.
- Appendix: Related Documentation: contains a list of all documentation published to support NetWrix Event Log Manager.

2. DEPLOYMENT OPTIONS

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.

If you wish to monitor computers that belong to several domains, you do not have to install several instances of NetWrix Event Log Manager (one per each domain). You can simply specify the credentials for collecting data from different domains (for details on how to specify these credentials, refer to Chapter 4.Configuring Managed Objects of NetWrix Event Log Manager Administrator's Guide).

3. INSTALLATION PREREQUISITES

This chapter describes the necessary prerequisites for the NetWrix Event Log Manager installation.

3.1. Hardware Requirements

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

Table 1: 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.*

3.2. Software Requirements

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

Table 2: Event Log Manager Software Requirements

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

3.3. Target Computers Requirements

The following requirements apply to Event Log Manager target computers:

Table 3: Target Machines Requirements

Component	Requirement
Operating System	• Windows 2000 or later • Red Hat Enterprise Linux 5, Ubuntu 11, Ubuntu Server 11 – predefined, ready-to-use platforms • Any Linux system using Syslog (events collection rules must be created manually)
Services	Make sure that the Remote Registry service is started.

3.4. Supported Microsoft SQL Server Versions

Microsoft SQL Server provides the Reporting Services that enable creating, viewing and managing reports based on data stored in a SQL database. NetWrix Event Log Manager uses SQL Server Reporting Services to generate reports.

To use the SSRS-based reports functionality, Microsoft SQL Server must be installed on a computer that can be accessed by NetWrix Event Log Manager.

SQL Server is not included in the product installation package and must be installed manually or automatically through the Reports Configuration wizard. When configuring NetWrix Event Log Manager, the following dialogue will pop up asking you whether you want to install and configure SQL Server automatically, or use an existing SQL Server instance (for details, refer to NetWrix Event Log Manager Administrator's Guide):

Figure 1: Reports Configuration Wizard

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, and so on. Note that maximum database size in SQL Server Express editions may be insufficient.

The following Microsoft SQL Server versions are supported:

Table 4: Supported Microsoft SQL Server Versions

Version	Edition
SQL Server 2005	• Express Edition with Advanced Services (SP3 or above) • Standard or Enterprise Edition
SQL Server 2008	• Express Edition with Advanced Services • Standard or Enterprise Edition
SQL Server 2008 R2	• Express Edition with Advanced Services • Standard or Enterprise Edition
SQL Server 2012	• Express Edition with Advanced Services • Standard or Enterprise Edition

For your convenience, we have provided instructions on the manual installation and configuration of the SQL Server for the Reporting Services to function properly. For details on how to install Microsoft SQL Server 2005/2008 R2 Express and configure the Reporting Services, refer to the following technical article: Installing Microsoft SQL Server and Configuring the Reporting Services.

For full installation and configuration details, refer to documentation provided by Microsoft.

4. INSTALLING NETWRIX EVENT LOG MANAGER

To install NetWrix Event Log Manager, follow the procedure below:

Procedure 1. To install NetWrix Event Log Manager

1. Download NetWrix Event Log Manager.
2. Run the setup package called elmfree_setup.msi (for the Freeware Edition) elmfull_setup.msi (for the Enterprise Edition).
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 shortcut will be added to your **Start** menu.

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

5. CONFIGURING TARGET COMPUTERS

This chapter explains how to configure your target computers for monitoring by NetWrix Event Log Manager. Refer to one of the sections below for details:

- Configuring Windows Computers
- Configuring Syslog-Based Platforms

5.1. Configuring Windows 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.

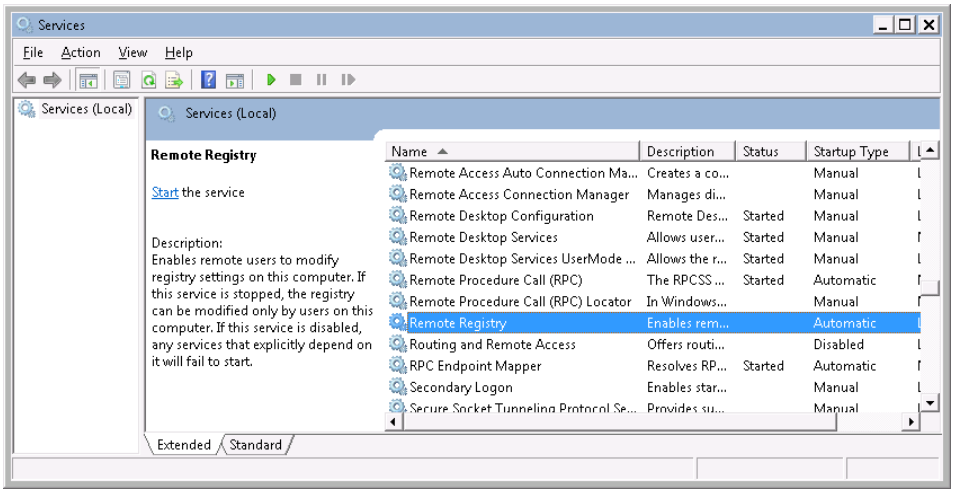
Verify that the service has been started on the computers that you want to monitor for events, otherwise run the service.

To enable the service, perform the following procedure:

Procedure 2. To enable the Remote Registry service

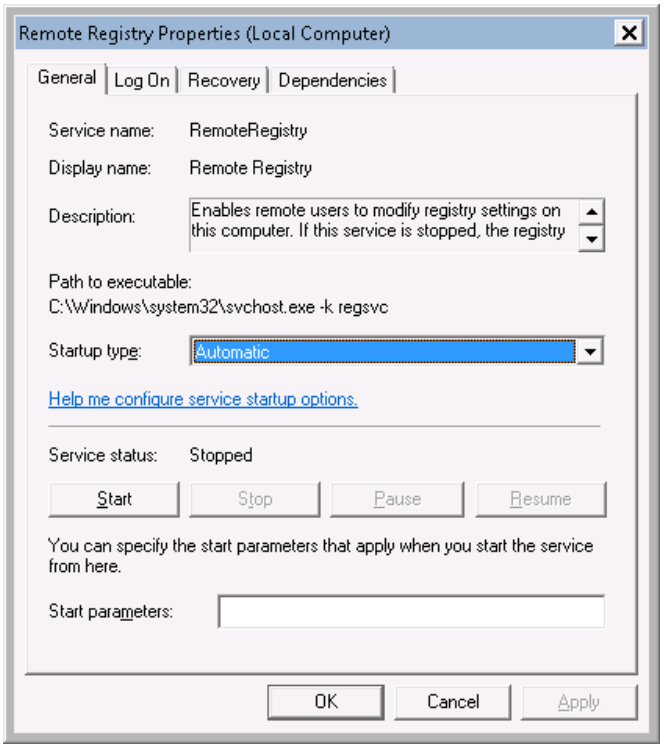
1. Navigate to **Start → Run.** Type `Services.msc` and click **OK.** In the **Services** dialog proceed to the **Remote Registry** service:

Figure 2: The Services Dialog



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 3: The Remote Registry Properties Dialog



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

5.2. Configuring Syslog-Based Platforms

To be able to process Syslog events, you must configure the Syslog daemon to redirect these events to the computer where NetWrix Event Log Manager is installed.

The procedure below explains how to configure redirection of the Auth log, as predefined Syslog-based platforms in NetWrix Event Log Manager have default rules to process this log only. You can create your own rules (for more information, refer to Section 7.6 Configuring the Syslog Platform Settings of NetWrix Event Log Manager Administrator's Guide) and configure redirection of events from other logs in the same way as described in the procedure below.

Procedure 3. To configure a Syslog daemon to redirect events

- For Red Hat Enterprise Linux 5:
  1. Open the /etc/syslog.conf file.
  2. Add the following line:

     `authpriv.* @FQDN/Netbios name` or `authpriv.* @ComputerIP`.

Note: `FQDN/Netbios name` and `ComputerIP` must be the name and IP address of the computer where NetWrix Event Log Manager is installed.

  3. Navigate to /etc/sysconfig/syslog file.
  4. Change the SYSLOGD_OPTIONS value to `SYSLOGD_OPTIONS="-r -m 0"`.
  5. Launch the RHEL console and execute the following command:

     `service syslog restart`

- For Ubuntu 11:
    1. Navigate to /etc/rsyslog.d/50-default.conf file.
    2. Add the following line:

       `authpriv.* @FQDN/Netbios name` or `authpriv.* @ComputerIP`
    3. Launch the UBUNTU console and execute the following command:

       `service rsyslog restart`

Note: `FQDN/Netbios name` and `ComputerIP` must be the name and IP address of the computer where NetWrix Event Log Manager is installed.

6. UPGRADING FROM PREVIOUS VERSIONS

To upgrade NetWrix Event Log Manager to the latest released version, perform the following procedure:

Procedure 4. To upgrade NetWrix Event Log Manager

1. Download the latest version of NetWrix Event Log Manager.
2. Open NetWrix Enterprise Management Console. Check the data collection status for each of your Managed Objects. If it is **OK** or **Completed with warnings and errors**, click the **Event Log Manager** node under this Managed Object and clear the **Enable the Event Log Manager** check-box. If it is **Running**, wait until the task completes and then disable the product.
3. Run the downloaded installation package.
4. Follow the steps of the installation wizard.

   Note: Do not change the program installation path on the **Destination Folder** step of the wizard, otherwise your current configuration may be lost.
5. At the end of the installation process, specify the credentials of the account that will be used by the product for data collection. You can specify the data processing account you used previously.
6. When the installation is complete, in NetWrix Enterprise Management Console select the **Enable the Event Log Manager** option for all of your Managed Objects.

   Note: All of your product settings will be preserved, and no reconfiguration is required.

7. UNINSTALLING NETWRIX EVENT LOG MANAGER

To uninstall NetWrix Event Log Manager from your computer, perform the following procedure:

Procedure 5. To uninstall NetWrix Event Log Manager

1. Navigate to **Start → Control Panel → Programs and Features**.
2. In the **Programs and Features** dialog, select **NetWrix Event Log Manager** and double-click it.
3. Click **Yes** in the confirmation dialog.

The program will be deleted automatically.

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 Installation and Configuration Guide	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 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 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 customers may experience while using the release version 4.0.