NETWRIX EVENT LOG MANAGER

USER 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 is intended for end users of NetWrix Event Log Manager. It contains information on different NetWrix Event Log Manager reporting capabilities, lists all available report types and report output formats, and explains how these reports can be viewed and interpreted.

This guide can be used by auditors, company management or anyone who wants to view audit reports on the monitored environment.

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 Reports: contains a full list of all available reports and explains how to view and interpret them.
- Chapter 3 Real-Time Alerts: provides a description and examples of real-time alerts.
- A Appendix: Related Documentation: contains a list of all documentation published to support NetWrix Event Log Manager.

2. REPORTS

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

The product provides a comprehensive set of predefined report templates that cover all aspects of the monitored environment and help you stay compliant with different regulations.

For a full list of reports provided by NetWrix Event Log Manager refer to Section 2.1 Reports List.

You can view reports through a web browser, or you can ask your system administrator to configure a subscription to the selected reports to receive them by email.

For details on these options, refer to the following sections:

- 2.2 Viewing Reports in a Web Browser
- 2.3 Receiving Reports by Email

2.1. Reports List

NetWrix Event Log Manager provides the following predefined reports:

Note: If none of these reports suit your needs, ask your system administrator to create cusom report templates, or order them from NetWrix.

Table 1: NetWrix Event Log Manager Reports List

Report Name	Description
Best Practice Reports	
Account Management	
Administrative Password Resets	Shows *when* account passwords were reset and *who* reset them.
Computer Account Changes	Shows computer accounts changes.
Group Management	Shows group changes.
Group Membership Management	Shows group membership changes.
Password Changes by User	Lists all password changes initiated by users. Password resets performed by administrators are not included in this report.
User Account Management	Shows changes to users' accounts.
Applications	
Service Installation Attempts	Shows service installation attempts.
Software Installation and Removal	Shows events related to software installation and removal.
Software Installation	Shows events related to software installation.
Software Removal	Shows events related to software removal.
Auditing	
Audit Log Cleared	Shows audit trail cleanup operations.
Audit Policy Changes	Shows changes to audit policy settings.
System Time Changes	Shows changes to system time.
User Account Locks and Unlocks	Shows user accounts lock and unlock events.
Computer Startups and Shutdowns	
All Planned Shutdowns	Shows planned shutdowns.
All Unexpected Shutdowns	Shows unexpected shutdowns.

DHCP Events	
All DHCP Server Errors	Shows all DHCP service errors, filtered by date range, computer name and user name.
All DHCP Server Events	Shows all DHCP service events, filtered by date range, computer and user name.
Logon Reporter	
Failed Logon Attempts	Shows failed authentication attempts in the Active Directory.
Remote Desktop Sessions	Shows remote desktop sessions, initiated, terminated, and reconnected.
Successful User Logons with Time Range	Shows user logons for a specified period of time.
Successful User Logons	Shows user logons.
User Logoffs	Shows user logoffs filtered by user name.
Service Control Manager	
All Service Errors	Shows all service errors, filtered by date range, computer and user name.
All Service Events	Shows all service events, filtered by date range, computer and user name.
All Service Starts	Shows all started services, filtered by date range, computer and user name.
All Service Stops	Shows all stopped services, filtered by date range, computer and user name.
Syslog	
Generic	
All Generic Events	Shows all syslog events of the Generic platform. The events are filtered by date range, computer and user name.
Red Hat Enterprise Linux 5	
Multiple Session Authentication Failures	Shows events generated after multiple failed attempts to open a session for Red Hat Enterprise Linux 5 in a row.
Session Authentication Failures	Shows failed attempts to open a session for Red Hat Enterprise Linux 5.
Sessions	Shows opening and closing of a session for Red Hat Enterprise Linux 5.
Ubuntu	
Multiple Session Authentication Failures	Shows events generated after multiple failed attempts to open a session for Ubuntu in a row.
Session Authentication Failures	Shows failed attempts to open a session for Ubuntu.
Sessions	Shows opening and closing of a session for Ubuntu.
General 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 Security Events by User	Shows all security events.
All System Events by User	Shows all system events.

The following sets of reports can be used if your organization needs to comply with certain regulations:

Table 2: Reports for Regulatory Compliances

Regulation	Reports List
GLBA	• Audit Log Cleared • Failed Logon Attempts • Successful User Logons • User Logoffs
HIPAA	• All Events by User • All Security Events by User • Audit Log Cleared • Audit Policy Changes • Computer Account Changes • Failed Logon Attempts • Group Management • Group Membership Management • Remote Desktop Sessions • Successful User Logons • System Time Changes • User Account Management • User Logoffs
PCI	• All Events by User • Audit Log Cleared • Audit Policy Changes • Failed Logon Attempts • Successful User Logons • User Logoffs
SOX	• All Events by User • All Security Events by User • Audit Log Cleared • Audit Policy Changes • Computer Account Changes • Failed Logon Attempts • Group Management • Group Membership Management • Remote Desktop Sessions • Successful User Logons • System Time Changes • User Account Management • User Logoffs

2.2. Viewing Reports in a Web Browser

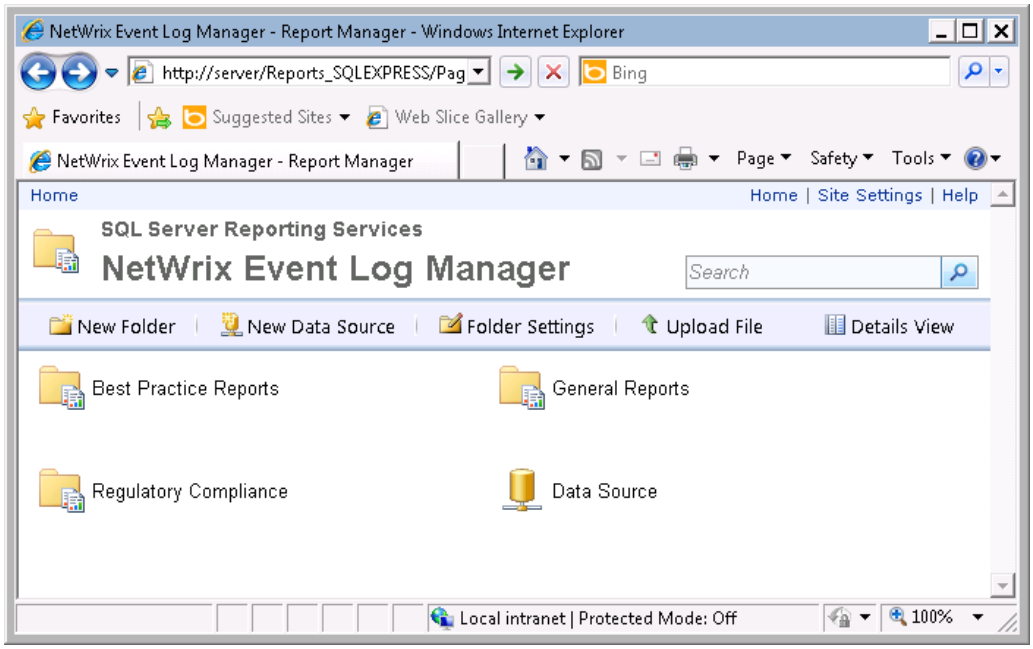
To view reports in a web browser, ask your system administrator to provide you with the Report Manager URL.

Perform the following procedure to veiw reports in a web browser:

Procedure 1. To view reports in a web browser

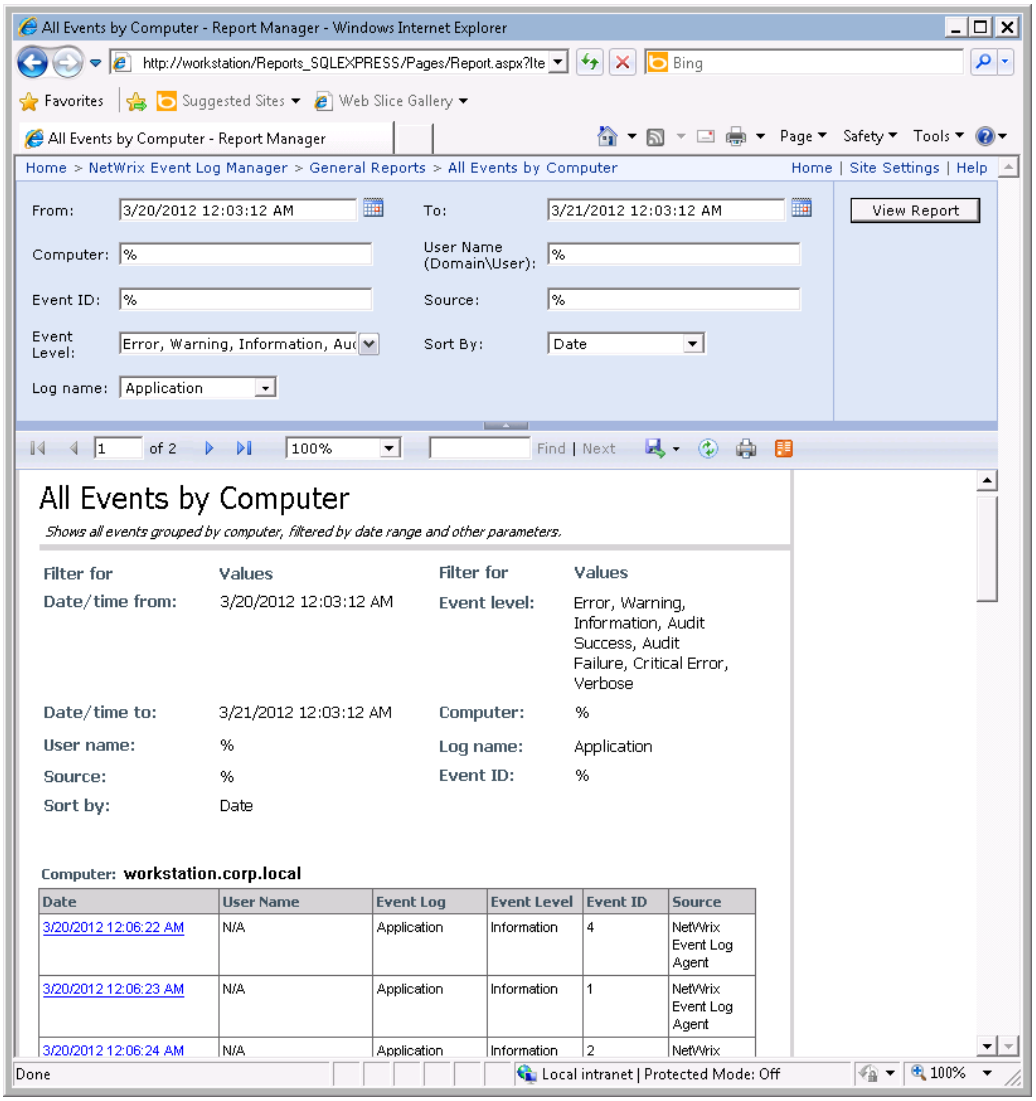
1. Open your web browser. Type the Report Manager URL in the address line and press **Enter.** The SQL Server Reporting Services **Home** page will open.
2. Click **NetWrix Event Log Manager**. The following page will open:

Figure 1: Report Manager: NetWrix Event Log Manager Page



3. All reports are divided into categories. Navigate to the required folder (for example, **General Reports → All Events by Computer**). On the page that opens, a report showing events for the last 24 hours will be displayed:

Figure 2: Report Manager: All Events by Computer Page



In the upper pane, you can specify filters that will be applied to collected events:

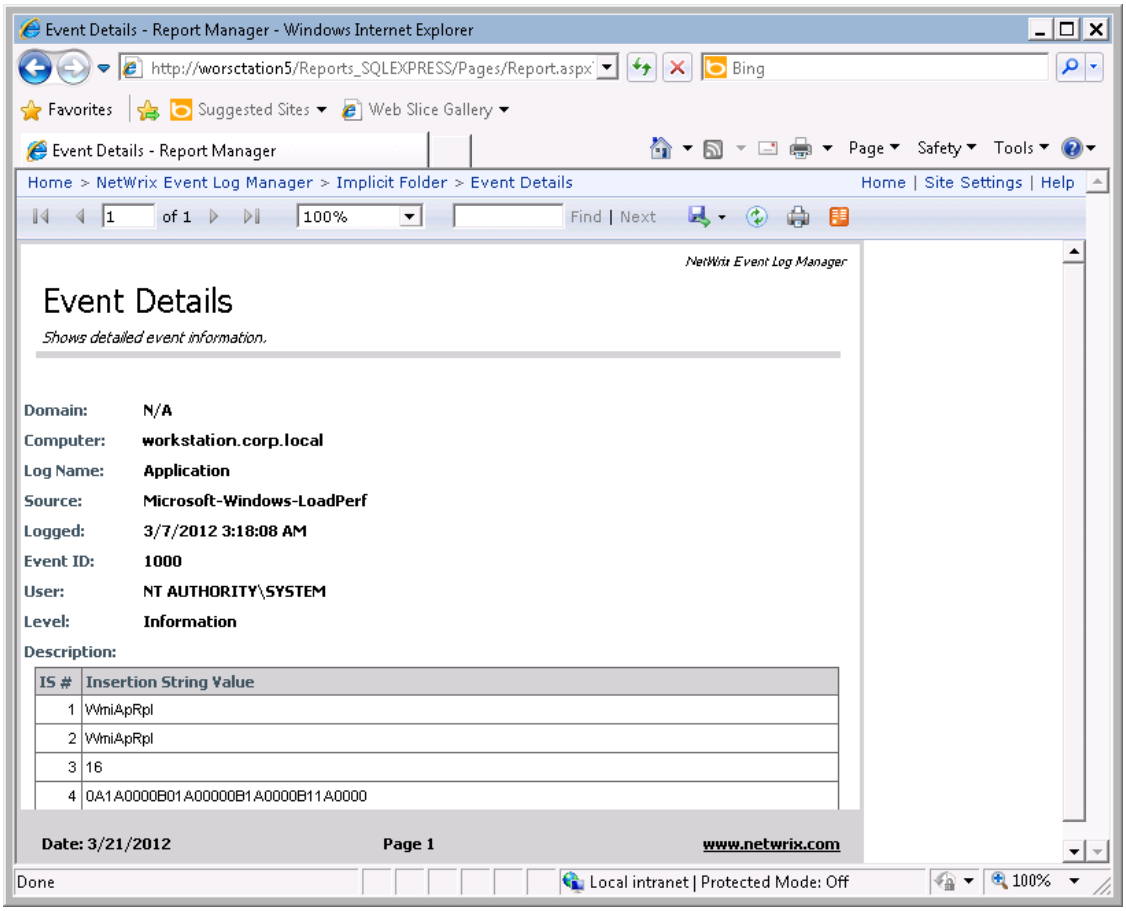
Note: The filters list may vary slightly depending on the report you have selected.

Table 3: Report Filters

Filter	Description
From	Specify the start date and time of the reporting period.
To	Specify the end date and time of the reporting period.
Computer	Specify the name of a computer if you want to display events from this computer only.
User Name (Domain\User)	Specify a user name. Only events generated under this account will be displayed.
Event ID	Specify the identifier of a specific event. Only events with this ID will be displayed in the report.
Source	Specify the name of a software product if you want to display events logged by specific software.
Event Level	Specify an event level to display events with this level only.
Log Name	Populate this field if you want to display events from a specific log.
Sort by	Specify a parameter that you want to sort events by.

4. To apply filters to a report, click the **View Report** button.
5. To view an event's details, click the link in the **Date** column of the corresponding event. The following page will be displayed:

Figure 3: Report Manager: Event's Details Page



2.3. Receiving Reports by Email

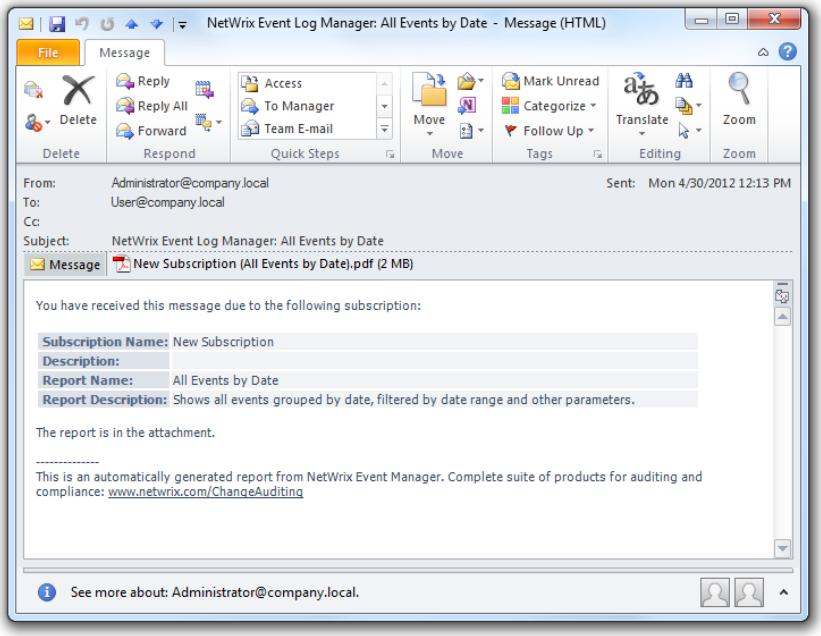
To receive reports by email, ask your system administrator to configure a subscription for you. You can ask the system administrator to configure filters to receive only the information you need and select the report output format: Excel, Word, or PDF.

Subscriptions can be delivered to you on one the following schedules:

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

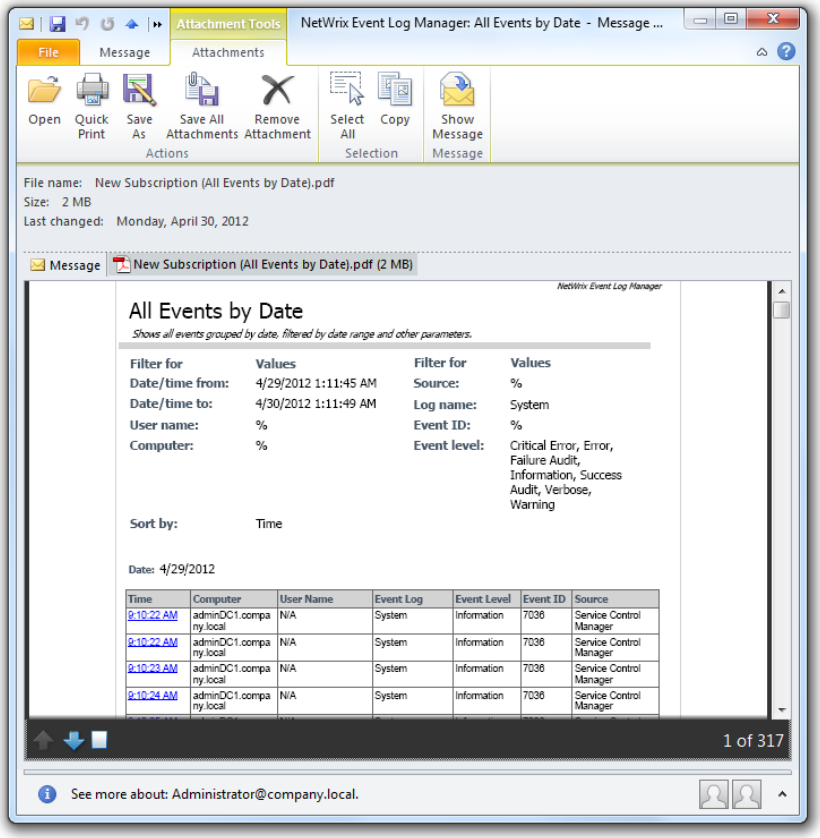
If you are subscribed to a report, you will receive an email like in the example below:

Figure 4: New Subscription



The report is attached to the email:

Figure 5: Attached Report



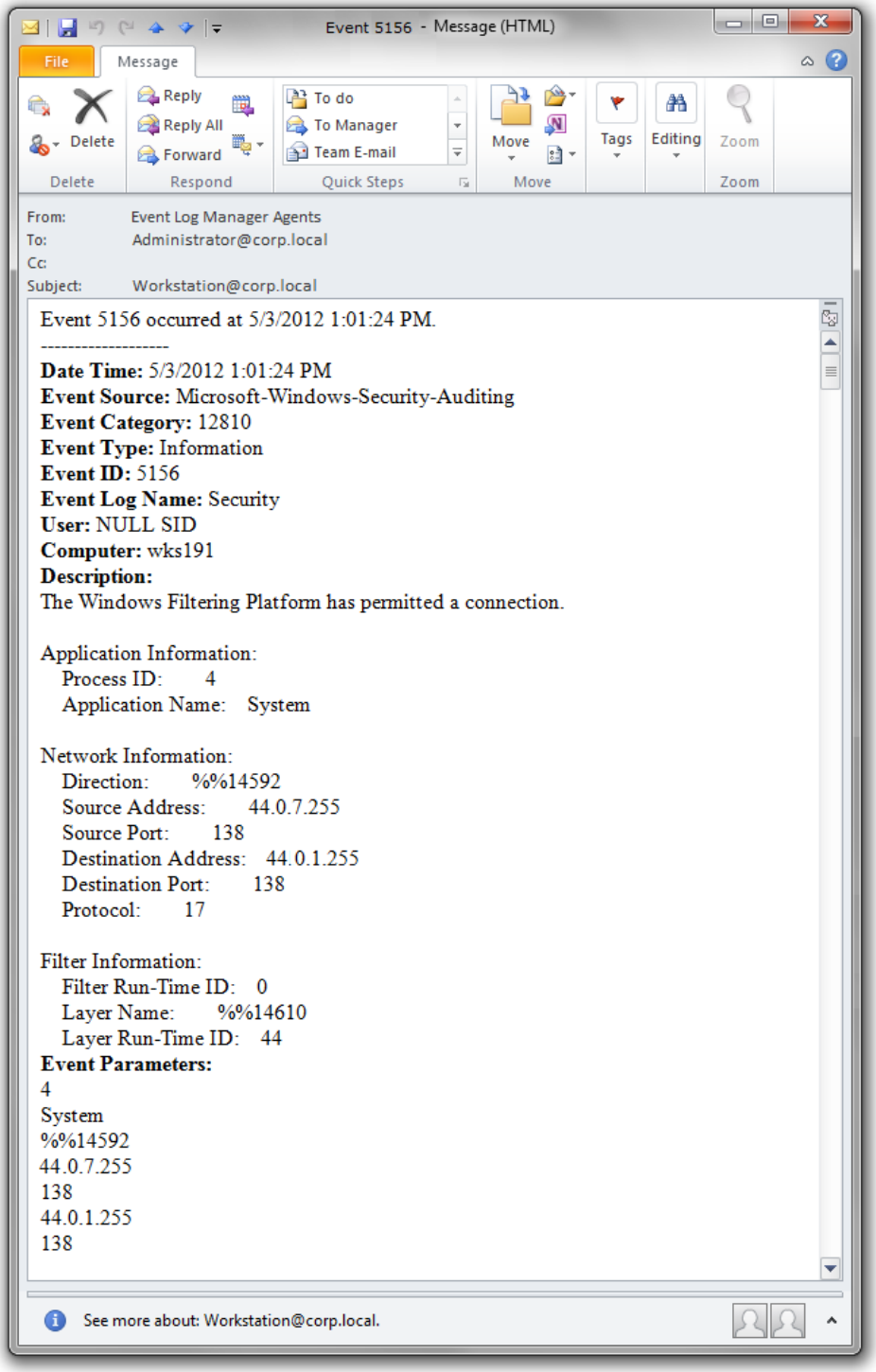
3. REAL-TIME ALERTS

Real-time alerts are notifications that can be configured to be triggered by certain events. After an event is detected, an email will be sent immediately to the specified recepients.

If you want to be notified about certain events, ask your system administrator to configure real-time alerts for you.

The example below shows a real-time alert informing you that the Windows Filtering Platform has allowed a program (source address 44.0.7.255) to connect to another process on the remote computer (desination address 44.0.1.255) on a UDP port (port 138).

Figure 6: Real-Time Alert Example



A real-time alert contains the following information:

Table 4: Real-Time Alert Fields

Field	Description
Date time	The date and time when the event was logged.
Event Source	The name of the software that logged the event.
Event Category	A number representing the event category defined by the Event Source.
Event Type	The type of the logged event.
Event ID	The unique identifier of the event.
Event Log Name	The name of the Event log containing the event.
User	An account under which the event was generated.
Computer	The name of the computer where the event was generated.
Description	Detailed information on the event.
Event Parameters	Event-specific information from the EventData field of the 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.

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 User Guide	The current document.
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 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 Release Notes	The document provides a list of known issues that customer may experience while using the release version 4.0.