# Contents

**About this Guide** ........................................................................................................................................ viii
- Purpose of this guide .............................................................................................................................. viii
- Who should read this guide.......................................................................................................................... viii
- Typographical Conventions .................................................................................................................... viii
- Document Revision Control .................................................................................................................... viii
- How to Get In Touch .................................................................................................................................... ix
- Documentation Support.................................................................................................................................... ix
- Customer Support........................................................................................................................................... ix

**Chapter 1 Getting Started** .................................................................................................................. 10
- About EventLogCentral................................................................................................................................. 11
- Prerequisites................................................................................................................................................ 13
- Starting EventLogCentral ............................................................................................................................... 13
  - Event-O-Meter ......................................................................................................................................... 19
- Switching Collection Point Sites ................................................................................................................... 20
- EventLogCentral Icons ................................................................................................................................. 20
- Viewing CAB Info.......................................................................................................................................... 22
- Accessing Shortcuts....................................................................................................................................... 23
- Incorporating your company logo................................................................................................................ 23
- Configuring EventLogCentral ....................................................................................................................... 24
- Searching Logs ............................................................................................................................................. 28
  - Basic Search.............................................................................................................................................. 28
  - Advanced Search....................................................................................................................................... 33
- Upgrading EventLogCentral License............................................................................................................ 45
- Exiting EventLogCentral ............................................................................................................................... 46
- Why Admin user credentials required for EventLogCentral authentication................................................ 49
- Is it mandatory for a user to have Administrator privileges to install EventLogCentral?............................ 49
- Can I install EventLogCentral with the user that does not have Administrator privileges?......................... 49
- Why Admin user credentials required for EventLogCentral authentication................................................ 49
- The pain of using non-admin credentials ................................................................................................... 50

**Chapter 2 Roles** ......................................................................................................................................... 51
- Roles ......................................................................................................................................................... 52
- Privileges................................................................................................................................................... 52
- Permissions ................................................................................................................................................. 52
- Viewing Role, Permissions and Privileges Assigned to Logged in User....................................................... 53
- Granting Permissions to users ..................................................................................................................... 54
- Viewing Unassigned Users ......................................................................................................................... 55
- Generating Report on Users ...................................................................................................................... 55
- Assigning Roles .......................................................................................................................................... 56
<table>
<thead>
<tr>
<th>Chapter 5 Analysis</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Analysis</td>
<td>131</td>
</tr>
<tr>
<td>Reg-ex Help</td>
<td>132</td>
</tr>
<tr>
<td>How to use Reg-ex</td>
<td>132</td>
</tr>
<tr>
<td>Help</td>
<td></td>
</tr>
<tr>
<td>What is a Custom</td>
<td>132</td>
</tr>
<tr>
<td>Column in the first</td>
<td></td>
</tr>
<tr>
<td>place?</td>
<td></td>
</tr>
<tr>
<td>What is the pressing</td>
<td>133</td>
</tr>
<tr>
<td>need for adding</td>
<td></td>
</tr>
<tr>
<td>Custom Columns in</td>
<td></td>
</tr>
<tr>
<td>Log Analysis?</td>
<td></td>
</tr>
<tr>
<td>How ELC helps?</td>
<td>134</td>
</tr>
<tr>
<td>Prior Knowledge</td>
<td>134</td>
</tr>
<tr>
<td>Components of</td>
<td>135</td>
</tr>
<tr>
<td>Custom Columns</td>
<td></td>
</tr>
<tr>
<td>What is Column Name?</td>
<td>135</td>
</tr>
<tr>
<td>Custom Column</td>
<td>135</td>
</tr>
<tr>
<td>Occurrences</td>
<td></td>
</tr>
<tr>
<td>What is Display</td>
<td>135</td>
</tr>
<tr>
<td>Name?</td>
<td></td>
</tr>
<tr>
<td>What is Separator?</td>
<td>136</td>
</tr>
<tr>
<td>What is Terminator?</td>
<td>136</td>
</tr>
<tr>
<td>Log Analysis -</td>
<td>136</td>
</tr>
<tr>
<td>Detail - On Demand</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6 Monitoring Enterprise Activities................................................................. 192

Standard column analysis................................................................................................. 136
Quick View ....................................................................................................................... 143
Custom column analysis.................................................................................................... 143

Log Analysis - Summary - On Demand........................................................................... 147
Standard column analysis................................................................................................. 147
Quick View (Smart Viewer).............................................................................................. 148
Custom column analysis.................................................................................................... 150

Log Analysis - Trend - On Demand.................................................................................. 151
Standard / Custom column analysis................................................................................ 151

Log Analysis - Detail - Queued......................................................................................... 154
Standard column analysis................................................................................................. 154
Custom column analysis.................................................................................................... 155

Log Analysis - Summary - Queued................................................................................... 157
Standard column analysis................................................................................................. 157
Custom column analysis.................................................................................................... 159

Log Analysis - Trend - Queued......................................................................................... 160
Standard column analysis................................................................................................. 160

Log Analysis - Detail - Scheduled.................................................................................... 162
Standard column analysis................................................................................................. 162
Custom column analysis.................................................................................................... 163

Log Analysis - Summary - Scheduled............................................................................. 164
Standard column analysis................................................................................................. 164
Custom column analysis.................................................................................................... 165

Log Analysis - Trend - Scheduled.................................................................................... 167
Standard column analysis................................................................................................. 167

Log Analysis - Detail - Defined........................................................................................ 168
Standard column analysis................................................................................................. 168
Custom column analysis.................................................................................................... 170

Resolving IP Address and viewing Event ID, Port details.................................................. 171
Viewing port details in EventTracker KB ......................................................................... 171
Resolving IP address......................................................................................................... 175

Viewing generated Queued Log Analysis...................................................................... 177
Searching generated Queued Log Analysis.................................................................. 177
Exporting summary report on generated Log Analysis..................................................... 177

Log Analysis Report queue statistics............................................................................ 178
Log Analysis queue statistics - Admin............................................................................ 178

Alert Analysis .................................................................................................................. 178
Alert Analysis - On Demand......................................................................................... 178
Quick View....................................................................................................................... 179
Alert Analysis - Queued.................................................................................................... 179
Alert Analysis - Scheduled.............................................................................................. 180

Tracking Alert Notification Status................................................................................ 181

Log Volume Analysis ..................................................................................................... 182

Log Volume Analysis - On Demand................................................................................ 182
Log Volume Analysis - Queued....................................................................................... 184
Log Volume Analysis - Scheduled................................................................................ 185

Suspicious Traffic Analysis............................................................................................. 186

Suspicious Traffic Analysis - On Demand...................................................................... 187
Suspicious Traffic Analysis - Queued............................................................................ 187
Suspicious Traffic Analysis - Scheduled...................................................................... 188

Cost Saving Analysis.................................................................................................... 189
Person Hour.................................................................................................................... 189
Monitoring Enterprise Activities ................................................................................................... 193
How it works .................................................................................................................................. 193
Enterprise Activity Dashboard ...................................................................................................... 193
Analyzing Enterprise Activity Volume ....................................................................................... 194
Analyzing per System Alerts ........................................................................................................ 197
Analyzing non-Admin User Activities ....................................................................................... 199
Analyzing Admin User Activities ............................................................................................... 206
Analyzing Activities per System ............................................................................................... 209
Analyzing IP Addresses by Traffic ............................................................................................. 210
Analyzing Processes by Occurrence ......................................................................................... 214
Analyzing Events by Occurrences .............................................................................................. 217

Chapter 7 Auditing Changes ................................................................................................. 219
What is Change Audit .................................................................................................................. 220
Prerequisite ............................................................................................................................... 220
Assessing Changes ..................................................................................................................... 220
Accessing Changes by Change Type .......................................................................................... 220
Authorizing Unauthorized Items ................................................................................................. 223
Viewing Access History................................................................................................................ 226
Viewing More Info on files ......................................................................................................... 229
Assessing Changes by Object Type ............................................................................................ 229
Assessing Configuration ............................................................................................................. 231
Viewing and Acting on Integrity Violations ................................................................................ 233
Scheduling Policy Comparison ................................................................................................... 234

Chapter 8 RSS Feeds ........................................................................................................... 237
RSS Feeds ................................................................................................................................. 238
Configuring Advanced Feeds ...................................................................................................... 238
Subscribing to RSS Feeds ........................................................................................................... 238
Add RSS feeds in RSS Reader ..................................................................................................... 246

Glossary ................................................................................................................................. 247
Index ...................................................................................................................................... 250
About this Guide

Purpose of this guide

This guide will enable you to use every option of EventLogCentral and provides detailed procedures for the same.

Who should read this guide

This guide is intended for:

- Administrators who are assigned the task of monitoring and maintaining the enterprise network using EventLogCentral
- Operations personnel who manage day-to-day operations using EventLogCentral

Typographical Conventions

Before you start, it is important to understand the typographical conventions used in this guide:

<table>
<thead>
<tr>
<th>This</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italics</td>
<td>References to other guides and documents.</td>
</tr>
<tr>
<td>Bold</td>
<td>Input fields, radio button names, check boxes, drop-down lists, links on screens, menus and menu options.</td>
</tr>
<tr>
<td>CAPS</td>
<td>Keys on the keyboard and buttons on screens.</td>
</tr>
<tr>
<td>{Text_to_customize}</td>
<td>A placeholder for something that you must customize. For example, {Server_Name} would be replaced with the name of your server/machine name or an IP address.</td>
</tr>
<tr>
<td>Constant width</td>
<td>Text that you enter, program code, files and directory names, function names.</td>
</tr>
<tr>
<td>⊳</td>
<td>A Note, providing additional information about a certain topic.</td>
</tr>
</tbody>
</table>

Table 1
Document Revision Control

This section defines the conventions followed for the document revision control number. The revision control number is an alphanumeric identifier, unique to the document. The components of the acronym identify the following:

- First three letters – name of the product
- Second two numbers – version of the product
- Third two numbers – build of the product
- Last four letters – document description

The document revision control number for this guide is as given below:

<table>
<thead>
<tr>
<th>Version</th>
<th>Build</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELC 3.5</td>
<td>30 USGD</td>
</tr>
</tbody>
</table>

Name of the Product

Document Description

The document revision control number for this guide is as given below:

<table>
<thead>
<tr>
<th>File Name</th>
<th>EventLogCentral v3.5 b30 User Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Updated in accordance with release version 3.5 build 30.</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Release Date</td>
<td>Feb 09, 2010</td>
</tr>
</tbody>
</table>
How to Get In Touch

The following sections provide information on how to obtain support for the documentation and the software.

Documentation Support

Prism Microsystems, Inc. welcomes your comments and suggestions on the quality and usefulness of this document. For any questions, comments, or suggestions on the documentation, you can contact us by e-mail at support@prismmicrosys.com.

Customer Support

If you have any problems, questions, comments, or suggestions regarding EventLogCentral, contact us by e-mail at support@prismmicrosys.com. While contacting customer support, have the following information ready:

- Your name, e-mail address, phone number, and fax number
- The type of hardware, including the server configuration and network hardware if available
- The version of EventLogCentral and the operating system
- The exact message that appeared when the problem occurred or any other error messages that appeared on your screen
- A description of how you tried to solve the problem
Chapter 1
Getting Started

In this chapter, you will learn about:

- EventLogCentral
- Prerequisites
About EventLogCentral

EventLogCentral is a Web-based, cross-browser compatible user interface for EventTracker.

New! Enterprise Activity Dashboard

Provides information about unusual behavior by:

- Continuously monitoring the event log stream
- Performing a combination of statistical and behavioral correlation
- Detecting both new activity and activities that significantly deviate from normal operations

Conditions detected include:

- Abnormally high or low admin and user activity
- Abnormally high or low system, process or IP activity
- First seen for IP addresses, admins, users, processes etc.
- Sudden changes in event volumes

New! Alerts Dashboard

New! Change Audit

Analyze configuration changes

- Minimize security risks caused by authorized and unauthorized changes
- Identify any changes in EXE, DLL, Drivers, INI files, registry and other configurations
- Reduce the time and cost associated with configuration changes
- Standardize server configurations

Analyze vulnerability

WhatChanged performs regular and automatic scanning of your systems – whether or not they are exposed to known vulnerabilities which may generate potential security risks for your environment.

EventLogCentral helps you:

- Analyze trend of events through Event-o-meter.
- Add Favorites.
- Schedule/Define/Run On Demand reports through Alphabetical Reports.
- View Report Snapshot.
- Add Custom Columns.
- Configure time interval in Advanced Reports.
Configure Trend Analysis Reports.

Analyze logs including arbitrary ranges like “events occurred within the specified time range”

Move users from one role to another role. Note that users assigned with EventTracker Admin role cannot change their roles.

Securely logon with user credentials to access different systems, network resources and applications. When the user logs in, the network identifies the user’s “Role” within the organization and the “Services” available from the network infrastructure, and then dynamically assigns a set of “Rules” based on the user’s role, making access control and application prioritization possible.

Comply with audit requirements for GLBA, HIPAA, Sarbanes-Oxley, FISMA, California Senate Bill 1386, the USA Patriot Act, NISPOM Chapter 8, and PCI Data Security Standard.

Analyze Logs.

Analyze Log Volume.

Analyze Suspicious Traffic.

Analyze Alerts.

Analyze ROI.

Generate Collection Point Site specific audit-ready compliance reports.

Switch Collection Point Sites without logging out of the session.

View status of the CAB files received from Collection Points.

Enable / Disable Role-based access control while installation.

Restrict users to access EventLogCentral modules and computer groups based on Roles.

Generate reports in text and chart or in text only format.

Generate reports with 3D charts such as Pie, Bar (OR) Line chart.

Customize header and footer text that you want to display in the generated report

Generate reports in MS Word, PDF (OR) HTML format.

Search event description by framing Regular Expressions.

Run instant On Demand reports.

Configure My Report Templates with most frequently used configuration settings. The idea is to configure once and run any time you wish.

View the time slots occupied by Scheduled Reports in the Report Calendar.

Add, modify and delete RSS Feeds.
Prerequisites

EventLogCentral provides two User Authentication options namely “Local Account” and “Active Directory”. You can select an appropriate option while installing ELC, through the EventLogCentral Configuration dialog.

If you want “Local Account” authentication, the user accounts and group accounts should preexist in the target computer. So, create user accounts and group accounts in the target computer before you attempt to install ELC.

If you want “Active Directory” authentication, the user accounts and group accounts should preexist in the Active Directory. So, create user accounts and group accounts in the Active Directory before you attempt to install EventLogCentral.

What is the significance of creating EventTracker Group and ELC Administrator Group user groups?

To log on to EventLogCentral, the user must be a member of EventTracker Group. To administer roles in EventLogCentral, the user should be a member of ELC Administrator Group.

EventLogCentral user authentication operates locally, that is confined to a particular computer or within Active Directory context. EventTracker Group and ELC Administrator Group must be created prior to installing EventLogCentral.

Starting EventLogCentral

To Start EventLogCentral

1. Click Start, point to Programs, and click Internet Explorer. Type the URL of EventLogCentral in the Address bar, and then click Go.

   (OR)

   Click Start, point to Programs, point to Prism Microsystems, point to EventLogCentral, and click EventLogCentral.

   (OR)

   Click EventLogCentral... on your desktop.

   EventLogCentral displays the Login Page with logs processed information.
The links at the right-upper corner of the login page helps you to accomplish various tasks with ease.

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="About" /></td>
<td>View about EventLogCentral. EventLogCentral displays the information in a pop-up window.</td>
</tr>
<tr>
<td><img src="image" alt="Contact" /></td>
<td>EventLogCentral moves you through the contact page in prismmicrosys Web site.</td>
</tr>
<tr>
<td><img src="image" alt="FAQs" /></td>
<td>EventLogCentral moves you through the elc/faq page in prismmicrosys Web site.</td>
</tr>
<tr>
<td><img src="image" alt="Help" /></td>
<td>Access the online help.</td>
</tr>
</tbody>
</table>

2 Type valid **Username** and **Password** in the relevant fields.

Both Username and Password are mandatory. EventLogCentral users are authenticated locally or against the Domain Controller. Only members of **EventTracker** user group are allowed to log on to EventLogCentral. EventLogCentral displays an error message if the user is not a member of EventTracker user group. Users do not have rights to change their credentials through EventLogCentral.

3 Select a skin from **Themes** drop-down list.
4. Select a Collection Point Site from **Collection Point** drop-down list and then click **GO**.

**Note**

This option is available only for EventTracker Collection Master Console type.

EventLogCentral displays the **Home** page.

**Figure 2 ELC Home page**

---

**Note**

To avail **Change Audit** feature you need to have WhatChanged installed on the EventLogCentral server.
Note

Alerts Dashboard under Home tab and Enterprise Activity Dashboard under Enterprise Activity tab are available only for EventTracker Collection Master Console type.
Logged in user information and server information are displayed at the right-upper corner.

Table 4

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image" alt="ETAdmin" /></td>
<td>View logged in User Information.</td>
</tr>
</tbody>
</table>

This feature available for collection master only.
### Chapter 1: Getting Started

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="#">Image</a></td>
<td>Name of the Collection Master / Collection Point Site, you have selected while logging in. Switch Collection Point Site.</td>
</tr>
<tr>
<td><a href="#">Image</a></td>
<td>Open Event-O-Meter.</td>
</tr>
<tr>
<td><a href="#">Image</a></td>
<td>View RSS feeds.</td>
</tr>
<tr>
<td><a href="#">Image</a></td>
<td>Log out of EventLogCentral.</td>
</tr>
</tbody>
</table>

EventLogCentral displays **"Number of members in 'EventTracker' group exceeded licensed users"** message while you login to EventLogCentral if the number of members in 'EventTracker' user group exceeds the number of user license you had purchased.

---

**Figure 6 ELC Home page**
Solution: Remove member(s) from EventTracker user group and restart ELCReceiver service for the changes to take effect. Number of member(s) in EventTracker user group should be less than or equal to the user license you had purchased.

You can also upgrade EventLogCentral to match with the number of members(s) in EventTracker user group. Contact sales@prismmicrosys.com to upgrade your license.

Event-O-Meter

Event-O-Meter is an analytical graphical chart that helps quickly visualize per port trends of events against specified time range. In addition, numerical data has also been provided in a tabular format.

- Click

EventLogCentral displays the Event-o-meter graph.

Figure 7 ELC Home page

Figure 8 ELC Home page
Switching Collection Point Sites

EventLogCentral allows you to switch Collection Point sites without logging out of the session.

To switch among Collection Point sites

1. Click the Collection Point link at the right-upper corner. EventLogCentral displays the “Site Information” pop-up window.

2. Select a Site from Connect To drop-down list and then click Apply. EventLogCentral switches to the selected Collection Point Site.

EventLogCentral Icons

EventLogCentral Icons represent EventLogCentral objects. These icons help you to identify the various objects used in EventLogCentral.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green Icon" /></td>
<td>CAB files received successfully by the Collection the Master.</td>
</tr>
<tr>
<td><img src="image" alt="Blue Icon" /></td>
<td>CAB files being received by the Collection Master.</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>🔄</td>
<td>CAB files not received successfully by the Collection Master.</td>
</tr>
<tr>
<td>🛠️</td>
<td>Audit Failure type events.</td>
</tr>
<tr>
<td>🔒</td>
<td>Audit Success type events.</td>
</tr>
<tr>
<td>✗</td>
<td>All Error events.</td>
</tr>
<tr>
<td>📝</td>
<td>All Information events.</td>
</tr>
<tr>
<td>📝</td>
<td>Calendar Control.</td>
</tr>
<tr>
<td>🔨</td>
<td>Click to view Previous event details.</td>
</tr>
<tr>
<td>🔨</td>
<td>Click to view Next event details.</td>
</tr>
<tr>
<td>📝</td>
<td>Reports with no review notes.</td>
</tr>
<tr>
<td>📝</td>
<td>Reports with review notes.</td>
</tr>
<tr>
<td>📝</td>
<td>Reports with no review notes.</td>
</tr>
<tr>
<td>📝</td>
<td>Reports with review notes.</td>
</tr>
<tr>
<td>🔍</td>
<td>Click to search generated reports.</td>
</tr>
<tr>
<td>🎯</td>
<td>Click to generate summary report on the generated reports and export into EXCEL format.</td>
</tr>
<tr>
<td>🔄</td>
<td>New reports yet to be processed.</td>
</tr>
<tr>
<td>🔨</td>
<td>Reports being processed.</td>
</tr>
<tr>
<td>🔴</td>
<td>Reports failed to generate.</td>
</tr>
<tr>
<td>📦</td>
<td>No data found for the generated report.</td>
</tr>
<tr>
<td>🎯</td>
<td>Reports generated successfully.</td>
</tr>
<tr>
<td>🔨</td>
<td>Click to refresh a page.</td>
</tr>
<tr>
<td>🗂️</td>
<td>Schedule reports that are configured with e-mail settings.</td>
</tr>
<tr>
<td>🔮</td>
<td>Favorites.</td>
</tr>
<tr>
<td>🛠️</td>
<td>Client logo. You can replace this logo at the right-upper corner with your company logo.</td>
</tr>
<tr>
<td>🕒</td>
<td>Event-O-Meter</td>
</tr>
</tbody>
</table>
Viewing CAB Info

This option helps you to view Collection Point site wise CAB file details.

To view CAB information

1. Click the **Cab Info** tab.

   EventLogCentral displays the “Cab Status View” page.

2. Select the Collection Point site from the **Client** drop-down list.
3. Select the Status from the **Cab Status** drop-down list.
4. Click **View**.

   EventLogCentral displays the “Cab Status View” page.

**Note**

WEBDOC1 is the system where EventTracker Collection Master Console is installed.
Accessing Shortcuts

- Click the Shortcuts tab.

EventLogCentral displays the shortcut menu.

Incorporating your company logo

This section helps you to incorporate your company logo into EventLogCentral.

To Incorporate Your Company Logo

1. Browse and locate `companylogo.gif` in the installation directory\images folder. For example: `C:\Inetpub\wwwroot\CWG01\images`, will contain the company logo.

2. Rename "companylogo.gif" as "et-logo1.gif"

3. Copy your company logo into that folder and then rename it as `companylogo.gif`.

4. Login to EventLogCentral. Find that the footprint image at the right-upper corner is replaced with your company logo.
Configuring EventLogCentral

EventLogCentral dialog box helps you

- Enter configuration details that you have skipped while installing EventLogCentral.
- Modify configuration details that you have entered while installing EventLogCentral.

Care should be taken in entering the details for it may lead to undesirable consequences.

To configure EventLogCentral

EventLogCentral installed on the server, where there is an instance of EventTracker Collection Master Console is up and running.

1. Click Start, point to Programs, point to Prism Microsystems, point to EventLogCentral, and then click Configure EventLogCentral.

   EventLogCentral displays the “EventLogCentral Configuration” dialog box.
2 Type valid **UserName** and **Password**.

3 Type the EventTracker Group name in the **EventTracker Group** field.

4 Type the ELC Administrator Group name in the **Group** field.

5 Type the **Session Duration**. The length of time a user is allowed to remain inactive. If there is no user interaction with the application after this period, EventLogCentral kills the session and logs out the user. Default session duration is 60 minutes.

6 Select a **User Authentication** option.
Note

EventLogCentral selects the Console Type: Collection Master check box by default. If you clear the check box and click Ok, then EventLogCentral does not display the option to select Collection Point Sites.

7 Click OK.

Note

EventLogCentral displays the Roles tab on the top navigation bar, only when the logged in user has administrator's privilege and Enable Role Management check box (EventLogCentral Configuration dialog) was selected while installing EventLogCentral.

To configure EventLogCentral

EventLogCentral installed on the system, where there is an instance of EventTracker Collection Point / Standard Console is up and running.

1 Click Start, point to Programs, point to Prism Microsystems, point to EventLogCentral, and then click Configure EventLogCentral.
EventLogCentral displays the “EventLogCentral Configuration” dialog box.

2 Type valid **UserName** and **Password**.

3 Type the EventTracker Group name in the **EventTracker Group** field.

4 Type the ELC Administrator Group name in the **Group** field.

5 Type the **Session Duration**. The length of time a user is allowed to remain inactive. If there is no user interaction with the application after this period, EventLogCentral kills the session and logs out the user. Default session duration is 60 minutes.

6 Select a **User Authentication** option.

7 Click **OK**.
Searching Logs

EventTracker LogSearch is Google-like search facility available for quick search of events, it supports simple string search to parameterized search. For more information refer “EventTracker Log Search” guide.

Basic Search

To do Basic Search

1. Click the Log Search option on the Home page.

   EventLogCentral moves you through the Log Search browser window.

Figure 15 Log Search
2 Click the **logs processed today** hyperlink to view all logs processed since 12:00 A.M. till current time.

![Log Search](image)

3 To do a Basic search, type the keyword in the text box and then click **GO** or press **ENTER** on your keyboard. Example: Log Type:1.

Results are fetched for the search criteria set.
By default, logs processed in 24 hours are displayed.

**Note**

Log Search results will be displayed as per the Permissions assigned on Systems/Groups to the non-admin users. Refine is also done on the search result according to the Permissions. However, Admin users can search logs of all monitored systems.

4. Click the hyperlinks against the Event IDs to view event details in the EventTracker Knowledge Base.
To drill down the result set, click **Refine** on the toolbar.

(OR)

Click the **Search** menu and then select the **Refine** option.

Note that the Refine results are displayed only when the search is over.
Note

EventLogCentral displays the events count within brackets against the refine entities.

6 Select / type the refine criteria in the appropriate fields. Example: Event ID: 7036. You can also set Time Range to refine and view events that occurred in a particular time frame.

7 Click **Refine**.

Results are fetched for the search criteria set.

8 Click **Back** on the toolbar to go back to the previous page(s).

Note

"Back" button is enabled only when you refine the result set.

9 Click **New Search** to do a new log search.

10 Click the **Analysis** menu for detailed analysis.
EventLogCentral displays the message box.

![Closing Log Search and redirecting to Log Analysis in the main window.](image)

**11** Click OK.

EventLogCentral moves you back to the "Log Analysis – > Detail" page.

![Advanced Search](image)

**Advanced Search**

To do Advanced Search

**1** Click **Advanced Search** in the home page.
CHAPTER 1

GETTING STARTED

Figure 23 Log Search

Table 6

<table>
<thead>
<tr>
<th>Valid Search String</th>
<th>Search Field(s)</th>
<th>Sample Match String</th>
</tr>
</thead>
<tbody>
<tr>
<td>all these words</td>
<td>Description</td>
<td>Process ID</td>
</tr>
</tbody>
</table>

Explanation: This query matches the Search Field(s) and returns the matching records that contain that contain “Process” and “ID”

SYMANTEC TAMPER PROTECTION ALERT
Target: C:\PROGRA~1\SYMANT~1\VPTray.exe
Event Info: Open Process
Action Taken: Logged
Actor Process: C:\Program Files\Prism Microsystems\EventTracker\Agent\etagent.exe (PID 1944)
Name: -
Path: C:\Program Files\Prism Microsystems\EventTracker\ETCorrel\ETCorrel.exe
Process identifier: 2088
User account: SYSTEM
User domain: NT AUTHORITY
Service: Yes
RPC server: No
IP version: IPv4
<table>
<thead>
<tr>
<th>Valid Search String</th>
<th>Search Field(s)</th>
<th>Sample Match String</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP protocol: UDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port number: 2544</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allowed: No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User notified: No</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>this exact wording or phrase</strong></td>
<td><strong>Description</strong></td>
<td><strong>Process ID</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Explanation: This query matches the Search Field(s) and returns the matching records that contain the exact phrase “Process ID”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A new <strong>Process ID</strong>: 308</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Image File Name: C:\Program Files\Prism Microsystems\EventTracker\evtProcessEcFile.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creator <strong>Process ID</strong>: 3840</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Name: WEBDOC1$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain: TOONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logon ID: (0x0,0x3E7)</td>
</tr>
<tr>
<td><strong>search in standard column</strong></td>
<td><strong>Standard column</strong></td>
<td>src:security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src: is Standard column</td>
</tr>
<tr>
<td></td>
<td></td>
<td>security is Value</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Explanation</strong>: This query matches the Search Field(s) and returns the matching records that contain the exact value searched for.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log Type: Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Failure Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category: 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event ID: 861</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source: <strong>Security</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain: NT AUTHORITY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer: WEBDOC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User: SYSTEM</td>
</tr>
<tr>
<td><strong>one or more of these words</strong></td>
<td><strong>Description</strong></td>
<td><strong>ESTAB OR 80</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process ID: 744 OR IP version: IPv4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Explanation</strong>: This query matches the Search Field(s) and returns the matching records that contain any one of the value searched for.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A process has exited:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Process ID</strong>: 744</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Image File Name: C:\Program Files\Prism Microsystems\EventTracker\evtProcessEcFile.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Name: WEBDOC1$</td>
</tr>
<tr>
<td>Valid Search String</td>
<td>Search Field(s)</td>
<td>Sample Match String</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Domain: TOONS</td>
<td>Logon ID: (0x0,0x3E7)</td>
<td></td>
</tr>
<tr>
<td>Name: -</td>
<td>Path: C:\Program Files\Prism Microsystems\EventTracker\ETCorrel\ETCorrel.exe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Process identifier: 2088</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User account: SYSTEM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User domain: NT AUTHORITY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service: Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RPC server: No</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>IP version: IPv4</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP protocol: UDP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port number: 2771</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allowed: No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User notified: No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>event id range</th>
<th>Standard column</th>
<th>ID: 800-900</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> This query matches the Search Field(s) and returns the matching records that contain range of event ids searched for.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Type: Security</td>
<td>Event Type: Success Audit</td>
<td></td>
</tr>
<tr>
<td>Category: 6</td>
<td>Event ID: 850</td>
<td></td>
</tr>
<tr>
<td>Source: Security</td>
<td>Domain: NT AUTHORITY</td>
<td></td>
</tr>
<tr>
<td>Computer: WEBDOC1</td>
<td>User: SYSTEM</td>
<td></td>
</tr>
<tr>
<td>Log Type: Security</td>
<td>Event Type: Failure Audit</td>
<td></td>
</tr>
<tr>
<td>Category: 5</td>
<td>Event ID: 861</td>
<td></td>
</tr>
<tr>
<td>Source: Security</td>
<td>Domain: NT AUTHORITY</td>
<td></td>
</tr>
<tr>
<td>Computer: WEBDOC1</td>
<td>User: SYSTEM</td>
<td></td>
</tr>
</tbody>
</table>

<p>| knowledge | <em><strong>Alerts</strong></em> |</p>
<table>
<thead>
<tr>
<th>Valid Search String</th>
<th>Search Field(s)</th>
<th>Sample Match String</th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td></td>
<td>Explanation: This query returns the records that match the selected Knowledge Category.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Query result:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standard Columns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log Type: System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category: 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event ID: 3202</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source: EventTracker</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer: WEBDOC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Detected Service &lt;EventTracker Scheduler&gt; is not running.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name: EventTracker Scheduler</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type: Service</td>
</tr>
</tbody>
</table>

**systems or groups:** By default, search is done in all systems. You can also select systems or groups by clicking select systems or groups hyperlink.

**But don't show Logs that have**

<table>
<thead>
<tr>
<th>any of these unwanted words</th>
<th>Description</th>
<th>Explanation: This query matches the Search Field(s) and returns the matching records that do not contain the value searched for.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Example #1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>search in standard column: id:3225</td>
</tr>
<tr>
<td></td>
<td></td>
<td>One or more of these words: iexplore.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Query result:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standard Columns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log Type: System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category: 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event ID: 3225</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source: EventTracker</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain: TOONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer: WEBDOC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User: susan</td>
</tr>
<tr>
<td>Valid Search String</td>
<td>Search Field(s)</td>
<td>Sample Match String</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event Description</td>
<td></td>
<td>Socket DELETED:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type: TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status: Deleted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local Address: webdoc1.Toons.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local Port: 2190</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Address: ISA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Port: 80 (http)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection active time: 96 secs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last known Connection State: ESTAB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process ID: 2224</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process Name: iexplore.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Image File Name: C:\Program Files\Internet Explorer\iexplore.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To filter out records that matches iexplore.exe or firefox.exe in event description, frame your query as search in standard column: id:3225 any of these unwanted words: iexplore.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Query result:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standard Columns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log Type: System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category: 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event ID: 3225</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source: EventTracker</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain: TOONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer: WEBDOC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User: susan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Socket DELETED:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type: TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status: Deleted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local Address: webdoc1.Toons.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local Port: 3167</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Address: POPEYE.TOONS.LOCAL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Port: 135 (eepmap)</td>
</tr>
<tr>
<td>Valid Search String</td>
<td>Search Field(s)</td>
<td>Sample Match String</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection active time: 49 secs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last known Connection State: ESTAB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process ID: 888</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process Name: svchost.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Image File Name: C:\WINDOWS\System32\svchost.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Records that match unwanted words (iexplore.exe</td>
</tr>
<tr>
<td>Example #2:</td>
<td></td>
<td>search in standard column: id:3225</td>
</tr>
<tr>
<td></td>
<td></td>
<td>One or more of these words: Local Port: 3167</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Query result:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standard Columns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log Type: System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Type: Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Category: 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event ID: 3225</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source: EventTracker</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Domain: TOONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer: WEBDOC1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User: susan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Socket DELETED:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type: TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status: Deleted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local Address: webdoc1.Toons.local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local Port: 2484</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Address: POPEYE.TOONS.LOCAL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Port: 445 (microsoft-ds)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection active time: 147 secs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last known Connection State: TIME_WAIT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process ID: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process Name: [System Process]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Image File Name: N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standard Columns</td>
</tr>
<tr>
<td>Valid Search String</td>
<td>Search Field(s)</td>
<td>Sample Match String</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>

- Log Type: System  
- Event Type: Information  
- Category: 2  
- Event ID: **3225**  
- Source: EventTracker  
- Domain: TOONS  
- Computer: WEBDOC1  
- User: susan  

**Event Description**  
Socket DELETED:  
Type: TCP  
Status: Deleted  
Local Address: webdoc1.Toons.local  
Local Port: **3167**  
Remote Address: POPEYE.TOONS.LOCAL  
Remote Port: 135 (epmap)  
Connection active time: 99 secs  
Last known Connection State: TIME_WAIT  
Process ID: 0  
Process Name: [System Process]  
Image File Name: N/A  

To filter out records that matches Local Port: 3167 or 2484 in event description, frame your query as  
search in standard column: id:3225  
any of these unwanted words: Local Port: 3167 || 2484  
Records that match unwanted words (Local Port: 3167 || 2484) are filtered out.  

**Example #3:**  
To filter out records that matches Local Port: 3167 AND Last known Connection State: TIME_WAIT in event description, frame your query as  
search in standard column: id:3225  
any of these unwanted words: Local Port: 3167 AND Last known Connection State: TIME_WAIT  

Query result:
<table>
<thead>
<tr>
<th>Valid Search String</th>
<th>Search Field(s)</th>
<th>Sample Match String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Columns</td>
<td>Log Type: System</td>
<td>Event Type: Information</td>
</tr>
<tr>
<td></td>
<td>Category: 2</td>
<td>Event ID: 3225</td>
</tr>
<tr>
<td></td>
<td>Source: EventTracker</td>
<td>Domain: TOONS</td>
</tr>
<tr>
<td></td>
<td>Computer: WEBDOC1</td>
<td>User: susan</td>
</tr>
<tr>
<td></td>
<td>Event Description</td>
<td>Socket DELETED:</td>
</tr>
<tr>
<td></td>
<td>Type: TCP</td>
<td>Status: Deleted</td>
</tr>
<tr>
<td></td>
<td>Local Address: webdoc1.Toons.local</td>
<td>Local Port: 3167</td>
</tr>
<tr>
<td></td>
<td>Remote Address: POPEYE.TOONS.LOCAL</td>
<td>Remote Port: 135 (epmap)</td>
</tr>
<tr>
<td></td>
<td>Connection active time: 49 secs</td>
<td>Last known Connection State: ESTAB</td>
</tr>
<tr>
<td></td>
<td>Process ID: 888</td>
<td>Process Name: svchost.exe</td>
</tr>
<tr>
<td></td>
<td>Image File Name: C:\WINDOWS\System32\svchost.exe</td>
<td>Records that match unwanted words (Local Port: 3167 AND Last known Connection State: TIME_WAIT) are filtered out.</td>
</tr>
</tbody>
</table>

**Time Range:** Select the time frame from the *Select Time Range* drop-down list. You can search logs anytime since the installation of EventTracker Pulse. You can also select date and time from the *Select Custom Time Range* drop-down lists.

2 Type the search criteria. Example: search in standard column: id:540
   By default, search is done for all EventTracker discovered systems/groups. You can also select systems/groups by clicking Select systems or groups hyperlink.

3 Click the *Select systems or groups* hyperlink.
EventLogCentral selects the **Systems** option by default.

**Note**

Systems/Groups are displayed as per the Permissions assigned to the non-admin users. However, for Admin users all monitored Systems/Groups are displayed.

4. Select the **Groups** option.
Select the **All Systems** check box.
6 Select the systems / groups appropriately and then click **OK**.

Selected systems / groups are displayed in the systems or groups field.

7 Select the **Time range**.

8 Click **Search**.

Events with ID 540 that occurred in the selected system for the selected time range are fetched by this query.
Upgrading EventLogCentral License

This option enables you to upgrade EventLogCentral from evaluation version to licensed version. In addition, helps to upgrade had you purchased a new license say for example to support more users.

To upgrade EventLogCentral License

1. Click Start, point to Programs, point to Prism Microsystems, point to EventLogCentral, and click Upgrade License.

EventLogCentral displays the “Upgrade License” dialog box.
2 Type Key1, Key2 and Serial #1 in the same order and then click OK.

Note

This upgrade is applicable only to the EventLogCentral version you have installed and not to upgrade from earlier version to the latest version.

Exiting EventLogCentral

This option enables you to log out of EventLogCentral.

To exit EventLogCentral

- Click

EventLogCentral logs you out gracefully.
When two users log in with same user credentials, the first user is logged out automatically and EventLogCentral allows the second user to create the session.
Note

When there is no user interaction for a specified amount of time, EventLogCentral logs out the user.

Figure 32 ELC Log out page

Note

EventLogCentral logs out if no role is assigned to the user.
Why Admin user credentials required for EventLogCentral authentication

Is it mandatory for a user to have Administrator privileges to install EventLogCentral?

Yes. It is highly recommended to install ELC with the user that is a member of “Administrators” user group on the target computer.

Can I install EventLogCentral with the user that does not have Administrator privileges?

No. You cannot install EventLogCentral with the user that does not have local administrator privileges on the target computer.

Why Admin user credentials required for EventLogCentral authentication

EventLogCentral provides two User Authentication options namely “Local Account” and “Active Directory”. While installing EventLogCentral, select an appropriate option through the EventLogCentral Configuration dialog and provide valid user credentials. EventLogCentral services will run under this account.
“Local Account” / “Active Directory” authentication: The user must be a member of “Administrators” user group on the computer where EventLogCentral is being installed.

The pain of using non-admin credentials

Note that, to install EventLogCentral the user should be a member of “Administrators” user group on the computer where EventLogCentral is being installed. If you plan to use domain user credentials, then add that user to the “Administrators” user group on the target computer. Failing to do so will abort EventLogCentral installation. This section substantiates why non-admin user credentials are not accepted while installing EventLogCentral.

1 The following folders should be granted "Full Control" permissions to the non-admin users.

- All folders and subfolders under EventTracker Install path.
- C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
- C:\WINDOWS\Temp
- If the Archives (where EventTracker archives are stored) & Reports (where copies of generated reports are stored) folders are not under EventTracker install path, then "Full Control" permissions should be granted explicitly on these folders.

2 After installing EventLogCentral, if the permission is changed to any of the above listed folders, then EventLogCentral stops working.

For example, in an organization a person delegated to manage EventLogCentral, installs and configures EventLogCentral and EventLogCentral works fine without any glitches. After some point in time another person takes charge, intentionally or unintentionally changes the permissions to any of the folders listed above. Now, EventLogCentral fails to work due to lack of mandated permissions.

Assigning and tracking permissions on folders is a complex and cumbersome process that eats up a sizeable amount of time and cost. Needless to say the time and cost involved in making support calls. To avoid such bottlenecks, and to make your environment hassle free, it is mandated to provide local admin user credentials while installing EventLogCentral.
In this chapter, you will learn how to:

- View Role assigned to logged in user
- Grant Permissions to users
- Assign Roles
- Add Roles
- Edit Roles
- Delete Roles
- Generate report on Users
- Delete Users
Roles

Role can be defined in terms of the authorization and obligation policies for a particular job function, which specify what actions the user is permitted or is obliged to do.

Fine-grained role-based security model secures the content of the application and the enterprise network at large.

Role-based access control is built into EventLogCentral. EventLogCentral comes with predefined roles that are optimal for any organization. EventTracker Admin and EventTracker Admin Readonly roles are available for managing roles.

You can also create custom roles, grant privileges and permissions as per your requirements.

Privileges

Privileges are the rights granted to roles to access EventLogCentral modules.

Permissions

Permissions are the rights granted to users to access computer groups.

Prior to installing EventLogCentral, create two Active Directory groups namely, EventTracker and EventTracker Admin. Only the users present in EventTracker user group are allowed to access the application. An administrator user group (EventTracker Admin) must exist in the Active Directory for the functioning of roles.

Create users and add them in EventTracker user group, if they are ordinary users.

Create users (example user: ETAdmin) and add them in both EventTracker and EventTracker Admin user groups, if they are administrators.

While installing, EventLogCentral selects the Enable Role Management check box in the Configuration dialog box. Roles can also be enabled after installing EventLogCentral through the configuration dialog available in the start menu (Start -> Programs -> Prism Microsystems -> EventLogCentral -> Configure EventLogCentral).

While installing, EventLogCentral prompts you to enter ELC Administrator Group. EventLogCentral selects EventTracker Admin user group by default. Only the users present in EventTracker Admin group can

- Create, configure, and modify roles.
- Grant / revoke privileges to roles.
- Assign roles to users.
- Grant / revoke permissions to users.

Also, has the permission to access all the computer groups in your enterprise.

You have to explicitly grant permissions to access computer groups for user(s) assigned pre-defined roles or user-defined roles other than EventTracker Admin role.
Points to remember:

1. You can assign only one role per user.
2. You cannot modify or delete privileges granted to EventTracker Admin role.
3. You cannot delete EventTracker Admin role.

Viewing Role, Permissions and Privileges Assigned to Logged in User

This option allows you to view the user information like display name, user logon name, last login time, server name, role assigned, permissions and privileges.

To view user information

1. Logon to EventLogCentral.
2. Click the user name on the title bar.
   EventLogCentral displays the “User information” window.

![User Information](image)
**Granting Permissions to users**

To grant permissions to users

1. Log on to EventLogCentral.
   
   EventLogCentral displays the Home dashboard.

2. Click the **Roles** tab.
EventLogCentral displays the “Assigned Users” page.

3 Click the user name in User Name column.
EventLogCentral displays “Assign Permissions” page.

**Note**

Since ETAdmin belongs to EventTracker Admin user group and is assigned EventTracker Admin role, EventLogCentral grants permissions on all the computer groups.

4 Select appropriate system group(s).
5 Click Update.
EventLogCentral displays the “Assigned Users” page.
6 Click View in the “Privileges” column.
EventLogCentral displays the “Assigned Privileges” page.

---

**Viewing Unassigned Users**

To view unassigned users
- Click Unassigned Users hyperlink to view users who are not assigned any roles.
EventLogCentral displays the “Unassigned Users” page.

---

**Generating Report on Users**

To generate report on users

1 Click to view Report on Users.
EventLogCentral displays “File Download” pop-up window.
2 Click Open.
EventLogCentral displays the report on users.
Assigning Roles

This option allows you to assign roles to users. If no role is assigned, then you will be automatically logged out.

To assign roles to users

1. Log on to EventLogCentral (example user: test3)
   
   EventLogCentral logs you out, since no role is assigned.
Log on to EventLogCentral (example user: ETAdmin). EventLogCentral displays the Home dashboard.

3 Click the **Roles** tab.
EventLogCentral displays the “Assigned Users” page.

4 Click the **Unassigned Users** hyperlink.
EventLogCentral displays the “Unassigned Users” page.

5 Click **Assign Role**
EventLogCentral displays the Manage Users -> Assigned Users page.
Figure 38 Assigned Users page

Table 7

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Users</td>
<td>Displays all the unassigned users.</td>
</tr>
<tr>
<td>Selected Users</td>
<td>Displays all the users assigned the role selected from the drop-down list above.</td>
</tr>
<tr>
<td>View Privileges</td>
<td>Select a Role and then click this hyperlink to view the privileges associated with that role.</td>
</tr>
<tr>
<td></td>
<td>Click to generate report on users.</td>
</tr>
<tr>
<td></td>
<td>Click to refresh the page.</td>
</tr>
</tbody>
</table>

6 Select a role from the Select a Role drop-down list. Example: IT Manager.

7 To view the privileges on the EventLogCentral modules for the selected role, click View Privileges.

EventLogCentral displays the Assigned Privileges in a pop-up window.
8 Select user(s) from the All users list and then click $\text{Next >>}$

EventLogCentral displays the "Selected Users" list with newly added user(s).

9 Click $\text{Next >>}$

EventLogCentral displays the "Permissions" page.
10 Select the system groups appropriately and then click **Submit / Update**.

EventLogCentral displays the Assigned Users page with the new configuration.
Changing Role Assigned to the User

This option helps you to change the role of the users. You cannot change the role of the users assigned with EventTracker Admin role.

To change role assigned to the user

1. Log on to EventLogCentral.
2. Click the Roles tab.
3. Click the hyperlink in the Role column against the user that you want to change Role.
EventLogCentral displays the “Change Role” page.

4. Select a new role from the drop-down list in the New Role column.
5. Click Change Role.
EventLogCentral displays the confirmation message box.

![Confirmation message box]

6 Click OK.

EventLogCentral changes the role assigned to the user and displays the “Assigned Users” page.

![Assigned Users page]

Adding Roles

This option allows you to add new roles and assign privileges to the newly added roles.
To add roles

1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.

2. Click the Roles tab.
   EventLogCentral displays the “Assigned Users” page.

3. Click the Manage Roles option.
   EventLogCentral displays the “Manage Roles” page.

4. Select a role from the list and then click **Privileges**. Example:
   1. EventTracker Admin. EventLogCentral displays read-only privileges page.
   2. EventTracker Admin Readonly. EventLogCentral displays editable privileges page.

5. Click **Add**.
   EventLogCentral displays the add roles page.
6 Type appropriate details in the **Role Name** and **Role Description** fields.

7 Click **Next>>**.

EventLogCentral displays the “Assign Privileges” page.

8 Assign privileges appropriately. Example: only **View** the **Home** page.

9 Click **Submit**.

EventLogCentral displays the message box.
10 Click OK.

EventLogCentral displays the “Manage Roles” page with the newly created Role.

11 Now, click the Manage Users option.

EventLogCentral displays the “Manage Users -> Assigned Users” page.

12 Click the Unassigned Users hyperlink.

EventLogCentral displays the “Manage Users -> Unassigned Users” page.

13 Click the Unassigned Users hyperlink.

EventLogCentral displays the “Manage Users -> Unassigned Users” page.

14 Click Assign Role.

15 Select the Role from the drop-down list. Example: ELCU.

16 Select the users (example: Test4) and then click Next >>

EventLogCentral displays the “Permissions” page.
17 Select the system group(s) and then click **Submit / Update**.
EventLogCentral displays the “Manage Users -> Assigned Users” page.

18 Login with the user name (Test4), who is assigned ELCU Role.
EventLogCentral displays the Home page.

**Note**
It is obvious that the user can view only the Home page. The user’s privilege on the EventLogCentral modules is restricted to Home page.

---

**Editing Roles**

This option allows you to edit role name, role description and the privileges assigned to the role.

**To edit roles**

1 Log on to EventLogCentral.
EventLogCentral displays the Home dashboard.

2 Click the **Roles** tab.
EventLogCentral displays the “Manage Users -> Assigned Users” page.

3 Click **Manage Roles**.

4 Select the Role (ELCU).
5 Click the name of the role in Name column. EventLogCentral displays the new roles page.

6 Edit appropriately and then click Next>>. (OR)

Click Privilege to edit only the privileges. EventLogCentral displays the “Assign Privileges” page.
7 Select the Privileges appropriately. Example: Select all privileges under Reports.

8 Click Update.
EventLogCentral displays the message box.

9 Click OK.
Login with “Test4” user credentials. “Test4” user can now view both the Home and Reports tabs.

---

**Deleting Roles**

This option allows you to delete roles. Before deleting a role, you have to remove all users assigned to that role. You cannot delete EventTracker Admin Role.

**To delete roles**

1 Log on to EventLogCentral.
EventLogCentral displays the Home dashboard.

2 Click the Roles tab.
EventLogCentral displays the "Manage Users -> Assigned Users" page.

3 Click Manage Roles.

4 Select the check box in the Delete column against the Role (ELCU).

5 Click Delete.
EventLogCentral displays the confirmation message box.
6 Click **OK**.

EventLogCentral displays the error page asking you to remove the users associated with the selected role.

7 Click **Manage Users**.

8 Select the check box against the user who is assigned ELCU role.
9. Click **Delete User**.

EventLogCentral displays the warning message asking you to remove the permissions associated with the selected user.

10. Click **OK**.

11. Click the name of the user in the **Name** column.

EventLogCentral displays the “Assign Permissions” page.

12. Remove the permissions and then click **Update**.

EventLogCentral displays the “Assigned Users” page.
13 Now, select the user and then click **Delete User**. EventLogCentral deletes the selected user.

14 Click the **Manage Roles** option.

15 Select the Role (ELCU) and then click **Delete**. EventLogCentral deletes the selected role.

**POINTS TO REMEMBER:**

- Remove all the permissions associated with the users.
- Delete all the users associated with Role.
- Delete the Role.

---

**Deleting Users**

This option allows you to delete users. Before deleting a user, you have to remove all permissions given to the user.
To delete users

1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2. Click the Roles tab.
   EventLogCentral displays the "Manage Users -> Assigned Users" page.
3. Select the check box in the Delete column against the user that you want to delete.
4. Click Delete User.
   EventLogCentral displays the confirmation message box.
5. Click OK.
   EventLogCentral displays the error message asking you to revoke the permissions first before you delete the user.
6. Click the user name in the User column.
   EventLogCentral displays the "Assign Permissions" page.
7. Clear all the check boxes in the Select column.
8. Click Update.
   EventLogCentral displays the "Manage Users -> Assigned Users" page.
9. Select the user and then click Delete User.
   EventLogCentral displays the confirmation message box.
10. Click OK.
EventLogCentral deletes the selected user.

**POINTS TO REMEMBER:**

- Remove all the permissions associated with the user.
- Delete the User.
In this chapter, you will learn how to:

- Interpret Alerts Summary
Home Overview

It serves you better if you understand the EventLogCentral interface in general and the menus, navigation links and the severity indicators in particular. This section elucidates how to work with EventLogCentral Home dashboard.

- Log on to EventLogCentral.
  ELC displays the Home dashboard.

Title Bar
Title bar displays the company logo at the right-upper corner, name of the logged in user, name of the server, logout button, and Server Time at the right-upper corner.

Top Navigation Bar
Top navigation bar consists of main options like Home, Enterprise Activity, Reports, Roles, Cab Info, Change Audit, and Shortcuts. EventLogCentral displays the Roles tab only for users with administrator privilege.

Bottom Navigation Bar
Bottom navigation bar consists of the corresponding options for the tabs in the top navigation bar.

Alerts Summary pane
Displays the name of the computer (System) where the Alerts originated, time and date (Time) when the Alerts originated, the source (Source) that caused the Alert to trigger and the event description (Description).

Alert Summary pane also displays the graphical representation of Alerts Summary. Each pie in the graph and the legend represents an Alert Rule.

Alerts Summary pane is not displayed when there are no Alerts generated in your enterprise network.
### Alerts Summary

Figure 63 Alerts Summary pane

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System group</td>
<td>Enterprise system groups are listed in this drop-down list. By default, EventLogCentral selects the ALL option.</td>
</tr>
<tr>
<td>Show systems top</td>
<td>By default, top 5 systems with more Alert events are displayed in the top pane. You can select up to top 20 systems.</td>
</tr>
<tr>
<td>Select the interval</td>
<td>Select the period for which you want to view Alert details.</td>
</tr>
</tbody>
</table>

Table 8

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Stacked Bar" /></td>
<td>View Stacked Bar graph.</td>
</tr>
<tr>
<td><img src="image" alt="Bar" /></td>
<td>View Bar graph.</td>
</tr>
<tr>
<td><img src="image" alt="Pie" /></td>
<td>View Pie graph.</td>
</tr>
<tr>
<td><img src="image" alt="Collapse" /></td>
<td>Collapse the top/bottom pane.</td>
</tr>
<tr>
<td><img src="image" alt="Expand" /></td>
<td>Expand the top/bottom pane.</td>
</tr>
</tbody>
</table>

Total alerts: Click this hyperlink to view all Alert events occurred in all monitored systems.

Table 9
Move the mouse pointer over the chart or the legend. EventLogCentral displays the Alert Rule along with the percentage of Alerts occurred under that rule.

1. Click the collapsible splitter controls to expand/collapse the panes.

By default, EventLogCentral displays the summary of events of top 5 Alert rules of the in the top pane.

2. Click a legend or a pie on the chart to view Alert details of that particular Alert rule.

EventLogCentral displays the “Alert Analysis” page.

3. Click Back at the upper-right corner to go back to the Home page.

4. Click Export to export all Alert details in Excel format.

5. Set the refine criteria, type the title of the Refine View and then click Refine.

EventLogCentral displays the details of latest 20 Alerts in the bottom pane.
Click the Total Alerts hyperlink in the bottom pane to view all Alert event details occurred in all monitored systems.

Click the name of the system in the bottom pane.

EventLogCentral displays the search result in the Log Search Browser.
8 Move the mouse over an event Id in the Event Id column. EventLogCentral displays the drop-down list.

9 Click Log Search to do a log search on the event id.

10 Click Knowledge Base to view event details in the EventTracker Knowledge Base Web site.
Chapter 4
Reports

In this chapter, you will learn how to:

- Configure Advanced Reports
- Configure My Reports
- Configure Advanced Feeds
- Configure My Feeds
- Interpret Reports Exceptions
- Configure Reports Settings
- Use Refine & Filter Options
- Define Reports
- View Report Calendar
- Create Favorites
Reports are arranged in alphabetical order to easily spot and configure On demand, Schedule, and Queue reports. Icons C, R, and A represent Categories, Miscellaneous Reports and Analysis respectively. Search option is provided to enter a free-form search query.

1. Click the Reports tab and then click the Alphabetical option. EventLogCentral displays the “Alphabetical reports” page.

2. Click the hyperlinks to view appropriate Category/Report/Analysis list.

   **Note**

   Search in results check box is not enabled when you click All.


4. Type the string you want to search, select the Search in results check box and then click Search. Example: alert

   EventLogCentral displays the Category/Reports/Analysis searched for.
5 Select a Report type.

6 Click Next>>.

EventLogCentral displays the Reports Wizard.

Note

You can also add Category/Reports/Analysis to the favorites list. To do this select a Category/Reports/Analysis and then click Add to Favorites.

---

**Advanced Reports and My Reports**

*Advanced* reports can be configured and viewed by any user who has access to EventLogCentral. Reports that are configured in EventTracker are also visible in Advanced Reports Dashboard.

*My Reports* can be configured and viewed only by the owner who configured those reports. No other user can view or modify My Reports. However, the administrator can view the configured reports and not the generated reports.

Procedure to configure On Demand, Queued and Scheduled reports are identical for both Advanced and My Reports.
Advanced Reports Dashboard

Advanced Reports Dashboard encompasses four panes namely Tree pane, Actions Pane, Advanced Dashboard pane and the Details pane.

Navigation Tree is an assortment of predefined report types. Reports of same type are grouped together for faster identification and navigation. Expand the nodes to select a report type that you wish to generate.

The Navigation Tree and the Navigation pane in the EventTracker Management Console work in tandem. The Category or Category Group that is displayed as "Not Installed" in EventTracker Navigation pane will also be displayed as "Not Installed" in the EventLogCentral Navigation Tree.

There are three tabs namely Compliance, Security and Operations are provided in the Tree pane. Compliance tab is selected by default and EventLogCentral displays compliance and certification related report types in the navigation Tree. Click Security and Operations tabs to view respective report types.

Whenever you define your own Category group(s) or Categories in EventTracker, EventLogCentral displays those user-defined entities under Operations -> User Defined Category group.
Actions pane contains related actions you can perform on the report type you have selected in the tree pane.

![Figure 72 Action pane](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the report.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the report.</td>
</tr>
<tr>
<td>Generated on</td>
<td>Date and time when the report was generated.</td>
</tr>
<tr>
<td>Size(kb)</td>
<td>Size in KB of the report.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the report such as Success, Failed and No record found.</td>
</tr>
</tbody>
</table>

Filters: You can use Duration or Status or combination of both to narrow down your search criteria.

<table>
<thead>
<tr>
<th>Display</th>
<th>Available options Summary and Exception. Summary is selected by default. Select Exception to move through the Exceptions page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Available options are Last One Hour, Last One Day, Last One Week and Last One Month.</td>
</tr>
<tr>
<td>Status</td>
<td>Available options are Show All, Success, Failed and No Record Found.</td>
</tr>
</tbody>
</table>

Select the “Show All” check box next to Report snapshot hyperlink to view all generated On Demand, Queued and Scheduled reports irrespective of the tab (Compliance, Security, Operations) selected in the Actions pane.

Report snapshot page displays the Overview and Queue status of the reports irrespective of the report type (Advanced and My Reports).
### Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users</strong></td>
<td>Select a user from this drop-down list to view the count of all reports configured by that user. EventLogCentral populates this drop-down list only when the logged in user has Admin privilege or Role Management is not enabled while installing EventLogCentral.</td>
</tr>
<tr>
<td><strong>ELC Configured only</strong></td>
<td>This check box is selected by default. Clear this check box to view reports configured in both EventTracker and EventLogCentral.</td>
</tr>
<tr>
<td><strong>Queue status</strong></td>
<td>Displays the queue status and Estimated Time to generate the report. You can also view the queue status by clicking Queued / On Demand Report in the Actions pane.</td>
</tr>
</tbody>
</table>

Details pane displays the configuration details and exception details of the report selected in the Advanced Dashboard pane. Click the title of the report in the Report Details tab to view the report. Click the Exception Details tab to view the exception summary of the selected report.

**To access Advanced Reports Dashboard**

1. Logon to EventLogCentral.
2. Click the **Reports** tab.
3. Click the **Advanced** option.
   
   EventLogCentral displays the Advanced Dashboard.

---

**My Reports Dashboard**

My Reports Dashboard encompasses four panes namely Tree pane, Actions Pane, My Dashboard pane and the Details pane.

Navigation Tree is an assortment of predefined report types. Reports of same type are grouped together for faster identification and navigation. Expand the nodes to select a report type that you wish to generate.
The Navigation Tree and the Navigation pane in the EventTracker Management Console work in tandem. The Category or Category Group that is displayed as "Not Installed" in EventTracker Navigation pane will also be displayed as "Not Installed" in the EventLogCentral Navigation Tree.

There are three tabs namely Compliance, Security and Operations are provided in the Tree pane. Compliance tab is selected by default and EventLogCentral displays compliance and certification related report types in the navigation Tree. Click Security and Operations tabs to view respective report types.

Whenever you define your own Category group(s) or Categories in EventTracker, EventLogCentral displays those user-defined entities under Operations -> User Defined Category group.

Actions pane contains related actions you can perform on the report type you have selected in the tree pane.
EventLogCentral displays summary in the My Reports Dashboard on all generated On Demand, Queued and Scheduled reports for the tab (Compliance, Security, Operations) selected in the Actions pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the report.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the report.</td>
</tr>
<tr>
<td>Generated on</td>
<td>Date and time when the report was generated.</td>
</tr>
<tr>
<td>Size(kb)</td>
<td>Size in KB of the report.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the report such as Success, Failed and No record found.</td>
</tr>
</tbody>
</table>

Filters: You can use Duration or Status or combination of both to narrow down your search criteria.

<table>
<thead>
<tr>
<th>Display</th>
<th>Available options Summary and Exception. Summary is selected by default: Select Exception to move through the Exceptions page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Available options are Last One Hour, Last One Day, Last One Week and Last One Month.</td>
</tr>
<tr>
<td>Status</td>
<td>Available options are Show All, Success, Failed and No Record Found.</td>
</tr>
</tbody>
</table>

Select the Show All check box next to Report snapshot hyperlink to view all generated On Demand, Queued and Scheduled reports irrespective of the tab (Compliance, Security, Operations) selected in the Actions pane.

Report snapshot page displays the Overview and Queue status of the reports irrespective of the report type (Advanced and My Reports).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Select a user from this drop-down list to view the count of all reports configured by that user.</td>
</tr>
</tbody>
</table>

EventLogCentral populates this drop-down list only when the
### Advanced Feeds

Advanced Feeds can be configured and linked with Advanced Reports to send RSS notifications when the scheduled Advanced Reports are generated. These feeds are configured in EventTracker and can be used by any user.

You cannot create, modify or delete Advanced Feeds through EventLogCentral.

#### To view Advanced Feeds

1. Log on to EventLogCentral.
2. Click the **Reports** tab.
3. Click the **Advanced** option.
   
   EventLogCentral displays “Advanced Reports” page.
4. Click **Advanced Feeds** in the Actions pane.
   
   EventLogCentral displays the “Advanced Feeds” page.
Table 14

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feed Name</td>
<td>Name of the RSS Feed.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the feed.</td>
</tr>
<tr>
<td>Added By</td>
<td>Name of the user who configured the feed.</td>
</tr>
<tr>
<td>Reports Linked</td>
<td>Click the links to view the reports linked with their corresponding feeds.</td>
</tr>
</tbody>
</table>

**5** Click the links in the **Reports Linked** column to view the corresponding reports linked to the selected feed.

EventLogCentral displays the “Advanced Feeds” page.

**My Feeds**

My Feeds can be configured and linked with My Reports to send RSS alerts when the scheduled My Reports is generated. My feeds are exclusive to the users who configure them.

You can create, modify or delete My Feeds through EventLogCentral.

**To add My Feeds**

1. Log on to EventLogCentral.
2 Click the **Reports** tab.

3 Click the **My Reports** option.

   EventLogCentral displays “My Reports” page.

4 Click **My Feeds** in the Actions pane.

   EventLogCentral displays the “My Feeds” page.

5 Click **Add New** to add new feeds.
Type appropriate details and then click **Save**.

**Table 15**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feed Name</td>
<td>Name of the RSS Feed.</td>
</tr>
</tbody>
</table>
## Reports Wizard

Reports Wizard has been designed to simplify the report generation and scheduling process by guiding you through a set of steps. You can select the report type, the systems, the time period and options and the data filters (if any).

Reports can be generated in PDF, HTML or WORD formats.

After the criteria are selected, the wizard presents an estimate of disk cost and time required for report generation. The estimate is based on past data.

## Reports Exceptions

Exceptions that occurred during report generation are displayed in this page. You can also add and clear follow up notes for the exceptions. Filtering options are provided to narrow down your search criteria.

1. Logon to EventLogCentral.
2. Click the **Reports** tab.
3. Click the **Advanced** option.

   EventLogCentral displays the Advanced Reports Dashboard.

   By default, EventLogCentral selects the first record in the top pane and displays the corresponding details in the bottom pane.

4. Click the **Exception Details** tab on the bottom pane.

   EventLogCentral displays the Exceptions details of the selected record.
To view all exceptions, click Exceptions on the Actions pane. EventLogCentral displays the “Exceptions” page.
### Table 16

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exceptions</td>
<td></td>
</tr>
<tr>
<td><strong>Generated on</strong></td>
<td>Date and time when the exception had occurred.</td>
</tr>
<tr>
<td>Exception name</td>
<td>Name of the exception.</td>
</tr>
<tr>
<td>Exception details</td>
<td>Summary of exception</td>
</tr>
<tr>
<td>Filter: You can use either one or both of these filter options.</td>
<td></td>
</tr>
<tr>
<td>Duration</td>
<td>Available options are Last One Hour. Last One Day. Last One Week. Last One Month. Select an option from this drop-down list to view respective exceptions.</td>
</tr>
<tr>
<td>Exception Type</td>
<td>Available options are Show All, flagged, Unflagged.</td>
</tr>
<tr>
<td></td>
<td>🔄 Represents Flagged exceptions. Flagged are ones that are with unattended comments.</td>
</tr>
<tr>
<td></td>
<td>□ Represents unflagged exceptions. Unflagged exceptions are ones that are with acknowledged comments or no comments.</td>
</tr>
</tbody>
</table>

Exceptions are raised under the following circumstances:

2. Report-processing time exceeds maximum allowed time (1 hour).
3. E-mail fails.

#### Flagging for follow up

- Click 🔄
  - EventLogCentral displays the Add Notes window.
  - Type the follow up note in the **Add new note** field and then click **OK**.

#### Clearing / acknowledging flags

- Click □
  - EventLogCentral displays the “Add Notes” window.
  - Type the follow up note in the **Add new note** field and then click **OK**.
  - Notes entered earlier are displayed in the “Notes” field.
Reports Configuration

Configuration options facilitate you to configure Published Reports backup directory, purge frequency and E-mail Configuration settings.

1. Click **Advanced / My Reports** option.
2. Click **Configuration** in the Actions pane.

![Configuration](image-url)
### Published Reports

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Backup Directory       | Folder to keep copies of generated reports. By default, EventLogCentral saves the reports in 
                         | …\Program Files\Prism Microsystems\EventTracker\Reports folder. You can select a different folder as you wish. |
| Purge Frequency        | Time schedule for the reporter to remove saved On Demand/Queued and Scheduled reports from the hard disk. Reports Console raises an event (2029) two days prior to deletion. EventTracker displays those events in the Dashboard of the Management Console. Clear the check boxes for the Reporter to retain all the reports forever. By default, Reporter will retain On Demand/Queued and Scheduled reports for 7 and 90 days respectively. You can configure these days from the spin boxes provided. |
| Prompt to publish on demand Quick View reports | On demand ‘Quick view’ reports are by default not published/saved on hard disk. This option will prompt you with an option to save/publish the report before closing. This check box is checked by default. |
Refine & Filter Options

Refine and Filter options in the Reports Wizard helps you to narrow down your filtering criteria while configuring reports.

Table 18

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate default report in case of no matching record found</td>
<td>Irrespective of the Report Format Type, EventLogCentral generates a pdf with the message &quot;No Matching Record Found.&quot; if there are no matching records found for the Queued or Scheduled reports / analyses</td>
</tr>
</tbody>
</table>

Table 19

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail Configuration: These are mandatory configuration settings for the ELC to &quot;Deliver report via E-mail&quot; or &quot;Notify report generation via E-mail&quot; upon generation of scheduled reports.</td>
<td></td>
</tr>
<tr>
<td>SMTP Server</td>
<td>Type a valid mail server name.</td>
</tr>
<tr>
<td>From e-mail id</td>
<td>Type a valid e-mail id.</td>
</tr>
<tr>
<td>Enable authentication</td>
<td>Select this check box and enter valid administrator user name and password.</td>
</tr>
<tr>
<td>To e-mail id</td>
<td>Type a valid e-mail id and then click Test E-mail to test the settings.</td>
</tr>
</tbody>
</table>

Refine: Use this option if you are looking for specific information.

Match for User(s)

This field can take multiple strings separated by ||. || Stands for OR condition.

Example: If you wish to generate a Log on/off Activity report for a specific user named "John" then, just enter John in the 'Match for User(s)' textbox. If you are looking for multiple users John, Leonard and Susan then, enter as John||Leonard||Susan.
### Field Description

| Match for specific information | This field can take multiple strings separated with && or ||. && Stands for AND condition and || stands for OR condition. If you want to make a match on any of the special characters like "", "^", "$", etc., then in the search string prefix this char with a backslash, like "\" for a "" and "\^" for a "^". Example: If you wish to generate a Printer Usage report for a specific printer named "FLR1PRINTER" then, just enter FLR1PRINTER in 'Filter for Specific Info' textbox. If you are wish to generate a Printer Usage report for a specific user "Susan", specific printer "FLR1PRINTER" and specific document "FinancialInfo.xls", you have to enter Susan in 'Match for User(s)' textbox and you have to enter FLR1PRINTER&&FinancialInfo.xls in 'Filter for Specific Info' textbox. |
| Filter: Use this option if you want to ignore specific information. |
| Filter User(s) | Type the user names to exclude from report generation. |
| Filter specific information | Type the information that you want to filter out in this field. Example. Suppose you want to generate software usage for a user and want to exclude all Microsoft applications from the report. Just enter Microsoft in this field. |

**Scheduled Reports**

To Configure Advanced scheduled reports

1. Logon to EventLogCentral.
2. Click the Reports tab.
3. Click the Advanced option.

EventLogCentral displays the Advanced Reports Dashboard.
Show all check box is selected by default. When this check box is selected, EventLogCentral displays all the generated reports in the top pane that includes On Demand, Scheduled and Queued irrespective of the tab (Compliance, Security, and Operations) and the report type selected. The corresponding details are displayed in the bottom pane.

Defining/scheduling using existing configuration

You can Define or Schedule reports/analyses with the same configuration settings of generated reports/analyses. To do this, select a generated report in the top pane and then select an appropriate option from the Use Configuration drop-down list. EventLogCentral starts the Reports Wizard.

- Select a generated On Demand report in the top pane.

EventLogCentral displays the corresponding details in the bottom pane.

Select an appropriate option from the Use configuration drop-down list. Example: Create defined report.
Click **GO**.

EventLogCentral starts the Reports Wizard.

---

Figure 84 Use Configuration

Figure 85 Use Configuration
Viewing Report Status

Report snapshot displays the Overview and Queue status of the reports irrespective of the report type (Advanced and My Reports). **ELC configured only** check box is selected by default. When this check box is selected, EventLogCentral displays on the reports configured in EventLogCentral. Clear this check box to view reports configured in both EventTracker and EventLogCentral.

- Click **Report Status** to view Report snapshot.

4. Click a tab in the navigation tree pane.
6. Click **Advanced Scheduled Report** in the Actions pane.  
   (OR)  
   Click **Scheduled** on the shortcut menu.  
   EventLogCentral displays the “Advanced Scheduled” page.
Table 21

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>Click the icon to add or view review notes.</td>
</tr>
<tr>
<td>Title</td>
<td>Name of the report. Click the title of the report to view the report.</td>
</tr>
<tr>
<td>Created on</td>
<td>Date and time when the report was created.</td>
</tr>
<tr>
<td>Size(kb)</td>
<td>Size in KB of the report.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the report such as Success, Failed and No record found.</td>
</tr>
</tbody>
</table>

Table 22

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>Search published reports.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refresh the pane.</td>
</tr>
</tbody>
</table>

Table 23

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled</td>
<td>Indicates that e-mail is configured.</td>
</tr>
</tbody>
</table>
If there are no reports scheduled or generated, then EventLogCentral displays the page with empty panes.

When no record is found, then EventLogCentral will not generate the output. To create a dummy PDF for the reports with no records, you need to select the **Generate default report in case of no matching record found** check box in the configuration page.

7 Click **New** in the Scheduled pane.

   EventLogCentral displays the Reports Wizard.

8 Click **Next >>**.
9 Select the **Chapters** (when applicable) and then click Next >>.

10 Select the **Categories** (when applicable) and then click Next>>.

11 Select Sites/Systems/System Groups.

12 Click Next >>.

13 Set the **Schedule Type**. Available options are Daily, Twice Daily and Weekly.

---

**Note**

If you select **Daily** and **Weekly** as Schedule Type, EventLogCentral displays the **Limit to time range** check box. By selecting this check box, EventLogCentral enables **From** and **To** spin boxes. Set the time range for EventLogCentral to consider events occurred during that period.

---

Figure 89 Limit to time range
Set the **Start Time**. Example: 12:00:00 PM

**Note**

EventLogCentral enables **Week Day** drop-down list only when you select **Weekly** option as Schedule Type.

Select an appropriate **Format option** (when applicable). Available options are Summary, Extended Summary, Details and Trend Analysis.

Select an appropriate **Export type** option. Available options are PDF, WORD and HTML.

Select an appropriate **Chart type**. Available options are PIE, BAR, LINE and NONE.

Select an appropriate **Sort by** option.

Click Next >>.

Type appropriate **Refine**, **Filter** options and then click Next >>.

Type the **Title**, **Header**, **Footer** and **Description**.

Crosscheck the Disk cost analysis details.

Select the **Enable publishing option** check box to deliver or notify results via E-mail. Type valid **To E-mail** address.

Select RSS Feed from the **Update status via RSS** to receive RSS notification.
25 Click Next >>.

26 Crosscheck the configuration and then click Schedule.
EventLogCentral adds the new schedule to the Scheduled pool.

Viewing Scheduled reports history and details

1 Click Advanced Scheduled in the Actions pane.
EventLogCentral displays the Advanced Scheduled page.

2 Click a title of the scheduled report in the bottom pane.
EventLogCentral displays the Report configuration details in the **Report details** tab.

3. Click the **History** tab to view report generation history.
Click a hyperlink in the Title column to view the generated report.

**Sending published reports via e-mail**

1. Click the icon in the top pane.
   
   EventLogCentral displays the “Send Report via Email” dialog box.
2 Type appropriately in the From, To, CC, and Subject fields and then click **Send**.

Running Scheduled Reports on demand

1 Select a report schedule in the bottom pane.
2 Click Run Now.

EventLogCentral displays the “Schedule run now” window.
**Table 24**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latest Scheduled Interval</td>
<td>Generate the saved report with latest scheduled interval.</td>
</tr>
<tr>
<td>Previous</td>
<td>Select this option to generate the report for the number of previous Day(s), Week(s) or Month(s) from the day of configuration of the selected report. The number of reports generated will depend on the Schedule option you have configured in the Report Option tab. For example, you have scheduled a daily report and have chosen to run the report for 1 month previous to the actual schedule; EventTracker will generate number of reports in proportion to the number of days in the previous month. If it’s a weekly report, EventTracker will generate reports in proportion to the number of weeks in the previous month. Say for instance 30 days 30 reports and 5 weeks 5 reports respectively.</td>
</tr>
<tr>
<td>Selected Day</td>
<td>Select this option to run the report for the day you select from the calendar control.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Selected Month</strong></td>
<td>Select this option to run the report for the selected month. The number of reports generated will depend on the number of days in the selected month.</td>
</tr>
<tr>
<td><strong>Selected Period</strong></td>
<td>Select this option to run the report for the selected period. Say for instance, if choose 7 days, EventTracker will generate 7 reports.</td>
</tr>
</tbody>
</table>

3. Select an appropriate option and then click **Generate**.

EventLogCentral displays the Disk Cost Analysis.

![Scheduled run now - Windows Internet Explorer](image)

4. Crosscheck the disk cost analysis and then click **Yes** to continue.

EventLogCentral displays the report generation progress.
On Demand Reports

On Demand reports can be generated in the foreground and background as well. Reports that are generated in the background are called Queued reports. On Demand page has two panes Overview and Queued.
Figure 99 Queued / On Demand reports

Table 25

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td>Click the icon to add and view review notes.</td>
</tr>
<tr>
<td>Title</td>
<td>Name of the report. Click the title to view the report.</td>
</tr>
<tr>
<td>Created on</td>
<td>Date and time when the report was created.</td>
</tr>
<tr>
<td>Size(kb)</td>
<td>Size in KB of the report.</td>
</tr>
</tbody>
</table>

Table 26

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Search published reports.</td>
</tr>
<tr>
<td></td>
<td>Refresh the pane.</td>
</tr>
</tbody>
</table>

Table 27

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the report.</td>
</tr>
<tr>
<td>Start</td>
<td>Date and time of the configured start time.</td>
</tr>
<tr>
<td>End</td>
<td>Date and time of the configured end time.</td>
</tr>
</tbody>
</table>
### Generating On Demand Reports – Foreground

This option helps to generate On Demand in foreground.

#### To generate Advanced On Demand reports in the foreground

1. Logon to EventLogCentral.
2. Click the **Reports** tab.
3. Click the **Advanced** option.
4. Click a tab. Example: Compliance.
5. Expand a reports node and select a report. Example: FISMA -> User Logoff.
6. Select the **On Demand** option from the shortcut menu.
   
   EventLogCentral displays the Reports Wizard.
7. Click Next `>>`.
10. Set the period for which you want the report to be generated. Example: Select the report generation interval: Last 2 Days.
11. Select the **Export type as Quick View**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured on</td>
<td>Date and time when the report was configured.</td>
</tr>
<tr>
<td>Updated on</td>
<td>Date and time when the report was modified.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the report such as New, Success, Under processing, Failed and No Record Found.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New On Demand</td>
<td>Configure a new report to generate in the foreground.</td>
</tr>
<tr>
<td>New Queued</td>
<td>Configure a new report to generate in the background.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit a report.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete a report.</td>
</tr>
<tr>
<td>Run now</td>
<td>Generate a report.</td>
</tr>
</tbody>
</table>

Table 28
12 Select the **Sort by** option.

13 Type appropriate Refine, Filter options and then click Next >>.

14 Type the **Title, Header, Footer, and Description**.

15 Click Next >>.

16 Crosscheck the Disk cost analysis details.

   EventLogCentral disables the Publishing options.

17 Click Next >>.

18 Crosscheck the Analysis parameters.

19 Click **Generate Report**.

   EventLogCentral displays the progress of report generation.

   EventLogCentral displays the generated report in the Power Viewer.
Click **Save to file** to export and save the report on your hard disk. EventLogCentral displays the “Export Crystal” dialog box.

21 Select the export type from the **Export Type** drop-down list.

22 Click **Yes**.

After saving the report, EventLogCentral displays the message box.
23 Click OK.

24 Click **Dashboard** in the Actions pane to view the report.

EventLogCentral displays the generated report and its details on the Dashboard.

---

**Generating On Demand Reports – Foreground – Power Viewer**

This option helps to generate On Demand in foreground. The generated report is displayed in the Power Viewer. With Power Viewer you can refine the result set by providing appropriate search criteria.

To generate Advanced On Demand reports in the foreground

1 Logon to EventLogCentral.
2 Click the Reports tab.
3 Click the Analysis option.
4 Click Details under Logs.
5 Select the On Demand option from the shortcut menu.
   EventLogCentral displays the Reports Wizard.
6 Click Next >>.
8 Select Sites/Systems/System Groups.
9 Set the period for which you want the report to be generated. Example: Select the report generation interval: Last 2 Days.
10 Select the Export type as Quick View.
11 Select the Sort by option.
12 Type appropriate Refine, Filter options and then click Next >>.
13 Type the Title, Header, Footer, and Description.
14 Click Next >>.
15 Crosscheck the Disk cost analysis details.
   EventLogCentral disables the Publishing options.
16 Click Next >>.
17  Crosscheck the Analysis parameters.

18  Click **Generate Report**.

   EventLogCentral displays the progress of report generation.

   EventLogCentral displays the generated report in the Power Viewer.

19  Type refine criteria to refine the result set and then click **Refine**.

20  Click **Export** to export and save the report on your hard disk.

   EventLogCentral displays the message box.

21  Click **OK**.

22  Click **Dashboard** in the Actions pane to view the report.
EventLogCentral displays the generated report and report details on the Dashboard.

Generating On Demand Reports – Foreground – Smart Viewer

Smart Viewer allows you to subtly refine the intricate result set with ease. Initially Smart Viewer displays the Summary, Extended Summary and then the Detailed view. Presently supports On Demand Category based reports (Summary & Extended Summary) and Log Analysis (Summary) based on Event Categories and Custom Properties.

To generate Advanced On Demand reports in the foreground

1. Logon to EventLogCentral.
2. Click the Reports tab.
   
   EventLogCentral displays the “Alphabetical” page.

   Icons C, R, and A represent Categories, Miscellaneous Reports and Analysis respectively.
3. Select a Category. Example: ***Alerts***.
   
   EventLogCentral selects the “On Demand” option by default.
4 Click Next >>.
5 Select Sites/Systems/System Groups.
6 Set the period for which you want the report to be generated. Example: Select the report generation interval: Last 2 Days.
7 Select the **Format option** as **Extended Summary**.
8 Select the **Export type** as **Quick View**.
9 Select the **Chart Type**.
10 Select the **Sort by** option.
11 Type appropriate Refine, Filter options and then click Next >>.
12 Type the **Title**, **Header**, **Footer**, and **Description**.
13 Click Next >>.
14 Crosscheck the Disk cost analysis details.
   EventLogCentral disables the Publishing options.

15 Click Next >>.
16 Crosscheck the Analysis parameters.
17 Click **Generate Report**.
   EventLogCentral displays the progress bar.
   After generating the report, EventLogCentral displays the Summary viewer based on the **Sort by** option you have chosen.
Click a record to view the Extended Summary.

Click a record in the Extended Summary to view the report in the Power Viewer.
Chapter 4: Reports

Generating On Demand Reports – Background (Queued)

To generate Advanced On Demand reports in the background:

1. Logon to EventLogCentral.
2. Click the Reports tab.
3. Click the Advanced option.
4. Click a tab in the navigation tree pane. Example: Compliance.
5. Expand a node and select a report type. Example: FISMA -> Track Application Access.
6. Click Queued / On Demand Report in the Actions pane.
7. Click New Queued in the Queued pane.
   EventLogCentral displays the Reports Wizard.
8. Click Next >>.
9. Select the Chapters (when applicable) and then click Next >>.

20. Click a hyperlink in the Event Id column to view event details in the EventTracker Knowledge Base.
10 Select the Categories (when applicable) and then click Next>>. Example: EventTracker: EXE tracking.
11 Select Sites/Systems/System Groups.
12 Set the period for which you want the report to be generated. Example: Select the report generation interval: Last 1 Day.
13 Select the Format option (when applicable).
14 Select an appropriate Export type.
15 Select an appropriate Chart type (when applicable).
16 Select an appropriate Sort by option.
17 Click Next >>.
18 Type appropriate Refine, Filter options and then click Next >>.
19 Type the Title, Header, Footer, and Description.
20 Click Next >>.
21 Crosscheck the Disk cost analysis details.
22 Select the Enable publishing option check box to deliver or notify results via E-mail. Type valid To E-mail address.
23 Select RSS Feed from the Update status via RSS to receive RSS notification.
24 Click Next >>.
25 Crosscheck the Analysis parameters.
26 Click Add to Queue.

### Defined Reports

Defined reports are tailor-made templates for the reports you often required to generate. Configure once and run as and when needed.

To configure Advanced defined reports

1 Logon to EventLogCentral.
2 Click the Reports tab.
3 Click the Advanced option.
4 Click a tab in the navigation tree pane.
5 Expand a node and select a report type. Example: PCI DSS -> Tracking User Activities.
6 Click Defined Reports in the Actions pane.
Click Defined on the shortcut menu.
EventLogCentral displays the Defined Reports page for the selected tab and report type.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the report.</td>
</tr>
<tr>
<td>Created on</td>
<td>Date and the time when the template was created.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select the check box and then click Delete to delete the report.</td>
</tr>
</tbody>
</table>

**Table 29**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Configure a new template.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit the template configuration settings.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected template(s).</td>
</tr>
<tr>
<td>Schedule</td>
<td>Add the selected template to run as schedule report.</td>
</tr>
<tr>
<td>Add to Queue</td>
<td>Add the selected template to run as on demand report in the background.</td>
</tr>
<tr>
<td>Run Now</td>
<td>Generate the report on demand in the foreground.</td>
</tr>
</tbody>
</table>

7 Click New.
EventLogCentral displays the Reporting Wizard.
8 Click Next >>.
9 Select the Chapters (when applicable) and then click Next >>.
10 Select the Categories (when applicable) and then click Next>>.
11 Select Sites/Systems/System Groups.
12 Set the period for which you want the report to be generated. Example: Select the report generation interval: Last 1 Day.
13 Select the Format option (when applicable).
14 Select an appropriate Export type.
15 Select an appropriate Chart type (when applicable).
16 Select an appropriate Sort by option.
17 Click Next >>.
18 Type appropriate Refine, Filter options and then click Next >>.
19 Type the Title, Header, Footer and Description.
20 Click Next >>.
21 Crosscheck the Analysis parameters.
22 Click Save.

Report Calendar

Report Calendar helps you to view the time slots occupied by the scheduled reports and to use the free slots efficiently for new schedule reports. Exploiting the free time slots enhances the performance of reports engine, which ultimately speeds up the report generation. Report Calendar displays the time slots of the current week starting from Monday through Sunday.

To access Report Calendar
1 Log on to EventLogCentral.
2 Click the Reports tab.
3 Click the Report Calendar option.

EventLogCentral displays the Report Calendar page.

Table 31

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Select a frequency from this drop-down list to view respective reports.</td>
</tr>
<tr>
<td>Time</td>
<td>View reports scheduled in that time slot.</td>
</tr>
<tr>
<td>Day</td>
<td>View reports scheduled on that day.</td>
</tr>
<tr>
<td>Show reports and analysis</td>
<td>EventLogCentral selects this check box and displays all reports and analysis schedules. Clear this check box and EventLogCentral displays only the reports schedules.</td>
</tr>
</tbody>
</table>

To view scheduled reports in a time slot
1 Click the links in the Time column.

EventLogCentral displays the reports scheduled in that time slot.
Table 32

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Title of the scheduled reports.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the scheduled reports.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Frequency of the report generation.</td>
</tr>
<tr>
<td>Scheduled Time</td>
<td>Date and time set for report generation.</td>
</tr>
<tr>
<td>Configured By</td>
<td>Name of the user who configured the report.</td>
</tr>
<tr>
<td>Comments</td>
<td>View read-only comments entered by the user.</td>
</tr>
<tr>
<td></td>
<td>□ indicates no comment had been entered by the user and □ indicates the user had entered comments.</td>
</tr>
</tbody>
</table>

2 Click □ in the Comments column.

EventLogCentral displays read-only Schedule Comments.

3 Click Close to close the Schedule Comments View.

To view scheduled reports on a day

- Click the name of the day.

EventLogCentral displays the reports scheduled on that day.

To view scheduled reports on a particular day and a time slot

- Click the links at the intersection of Day and Time columns, which is highlighted in red.

EventLogCentral displays the reports scheduled on that day and time slot.
Favorites

Favorites are bookmarks to often generated on demand Reports. A Report/Category/Chapter can be added to Favorites. You can also add Analysis to favorites list.

Adding to Favorites

1. Click the Reports tab.
2. Click the Advanced option.
3. Click a tab.
4. Expand a node and then click a report type.
5. Click Add to favorites on the shortcut menu.

EventLogCentral adds the report type to the favorites list and displays the Advanced reports page.

Viewing the favorites list

1. Click Favorites on the bottom navigation bar.

EventLogCentral displays the “Favorites List” pop-up window.

2. Select a Category and then click Generate Report to generate on demand report.
In this chapter, you will learn how to:

- Analyze Logs
- Analyze Log Volume
- Analyze Alerts
- Analyze Alert Notification Status
- Analyze Suspicious Traffic
- Analyze ROI
- Use Reg-ex Help
Log Analysis

Filter and display event logs based on user-defined criteria. The user can define the filter (or exclude) string as well as specify the output format.

Usage: Forensic Analysis of specific events, broad searches per criteria with subsequent sorting and ordering of the result set.

Reg-ex Help

Use this option to query using regular expressions. Complex expressions can take longer.

"Use the Wizard" to build the regular expression string used in the "Match for specific information" and "Filter specific information" fields.

How to use Reg-ex Help

1. Click the Advanced option in the Refine and Filter criteria page.
2. Click the Wizard hyperlink. EventLogCentral displays the Regular Expression Builder.
3. Type the expression you want to search in the Regular Expression field.
4. Select appropriately in the "Character and Repetition class" "Special Characters" "Groups and Options" tabs.
5. Click the Verifier tab.
6. Type the sample text in the Sample Input field.
7. Click Verify Expression.

EventLogCentral displays “Expression Matched” if the sample text matches or “Expression not Matched” if the sample text does not match in the Match Expression field.
What is a Custom Column in the first place?

To be precise, Custom Columns are user-defined columns. Aside from the standard report definition format, EventTracker reports module provides a simple, yet powerful log analysis reporting facility. It helps to parse and include parts of clogged SYSLOG like messages and Windows event descriptions as columns in reports. Custom Columns help you define new columns, bind it with the dynamic report templates and generate log analysis reports. EventTracker displays the parsed data under those columns defined by you.
While configuring Log Analysis, you can also choose the columns you are interested in, apply filters, sort columns, and rearrange the order of the columns that should appear in reports.

To put it in a nutshell Custom Columns help to manipulate data and generate comprehensible reports.

**What is the pressing need for adding Custom Columns in Log Analysis?**

Scouring the ingredients of Log data is massively time consuming and incredibly a painful task. The discovery process is analogous to finding a needle in a haystack.

Data contains pieces of information. Data will be meaningless if it is not understood, associated, and interpreted.

Since valuable information is dumped in the log description, there should be a way to break down and analyze the data and turn it into valuable business information.

Furthermore, there is no standardized message format as various vendors of NIX systems follow different conventions.

For example, comma-separated values, fixed-width text, and free-form text. It is difficult even for a seasoned administrator to decipher Syslog messages.

**How ELC helps?**

A common question that arises would be, “is it not sufficient to generate Log Analysis reports with templates provided with EventTracker?”

Is EventTracker flexible enough to add columns?

If so, does not EventTracker provide any predefined columns to simplify my work?

Is it possible to define my own columns?

If you’re preoccupied with these questions, relax!

EventTracker is shipped along with a precisely defined set of columns for your convenience. Should you wish to add columns if these predefined columns do not align with your requirement, EventTracker provides adequate facilities to add/modify/delete columns. Otherwise, default columns are sufficient.

If I bind new columns to the template, will those columns be saved permanently in the database?

It’s left to your discretion. While defining new columns, you’ve the luxury of saving the columns permanently in the database or binding the columns just for one instance of report generation.
Prior Knowledge

It is appreciable to have comfortable knowledge and understanding of Syslog message formats of different flavors of NIX systems. Though the fundamental tenets insist on simplicity, the creators of SYSLOG write the messages according to their whim and caprice. So suit yourself to the environment you work in to understand the syntax and semantics of Syslog messages.

Components of Custom Columns

Components of Custom Columns are the basic elements that are essential in framing your queries to extract required data from log messages.

What is Column Name?

Column Name is the “key” that reporter engine regards as a reference point and considers the string that succeeds for parsing. It is optional to provide column name and can contain:

- characters a,b,c…
- numbers 1,2,3…
- special characters #,$,%, space character…
- or combination of all three a1#

Custom Column Occurrences

If there are multiple occurrences of Column Name in the description, reporter engine considers only the first occurrence as reference point. So, be specific while you frame your query.

What is Display Name?

Display Name is a temporarily assumed name (alias) for the queried string. This name will appear as column title in the report. It is mandatory to provide display name and should be unique throughout the report. You can choose any name and can contain:

- characters
- numbers
- or combination of these two
- special characters are not accepted
What is Separator?
Separator is the “key” that reporter engine regards as a reference point and considers the string that succeeds for parsing. It is optional to provide separator and can contain:
- characters
- numbers
- special characters
- or combination of all three

What is Terminator?
Terminator is the “key” that reporter engine regards as a reference point and considers the string that precedes for parsing. The queried string is extracted till the first occurrence of the terminator. It is optional to provide terminator and can contain:
- characters
- numbers
- special characters
- or combination of all three

Thus, Custom Columns offer the flexibility to customize:
- data selection
- sort sequences
- column position

Log Analysis - Detail - On Demand

Standard column analysis
1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2. Click the **Reports** tab.
3. Click the **Analysis** option.
4. Click **Logs** in the Analysis tree.
   EventLogCentral displays the Logs Dashboard.
If there are no generated analyses, then EventLogCentral displays the page with empty panes.

You can **Define** or **Schedule** reports/analyses with the same configuration settings of generated reports/analyses. To do this, select a generated report in the top pane, select an appropriate option from the **Use Configuration** drop-down list and then click **Go**. EventLogCentral starts the Reports Wizard.
5 Click On Demand in the Actions pane.
   EventLogCentral displays the Reports Wizard.

6 Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.

7 Select the Select an event category option.

8 Select the Categories.

9 Click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.

10 Select the system(s) / group(s) / site(s).
   EventLogCentral displays the “Interval and More Options” page.

11 Select the Format option as Detail.

12 Select the report generation Interval.

13 Select the Export type.

14 Select the Sort by option.

15 Type the Refine and Filter criteria.
Figure 117 Refine and Filter
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Search</td>
<td>Use this option for simple queries (to use regular expressions, go to &quot;Advanced&quot;). The 'Refine' option is inclusive. Results are limited to matching entries. The 'Filter' option is exclusive. Results do not include matching entries. Any combination of Refine and Filter may be used simultaneously. Examples: Match for User(s): Enter usernames separated by</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Use this option to query using regular expressions. Complex expressions can take longer. &quot;Use the Wizard&quot; to build the regular expression string used in the &quot;Match for specific information&quot; and &quot;Filter specific information&quot; fields.</td>
</tr>
</tbody>
</table>

16 Select the **Advanced** option.
EventLogCentral disables **Match for User(s)** and **Filter User(s)** fields.

You can construct query to **Match for specific information** or **Filter specific information**.

17. Click the **Wizard** hyperlink.

EventLogCentral displays the Rx-Ex Help Wizard.
Type the expression you want to search in the Regular Expression field.

Select appropriately in the "Character and Repetition class" "Special Characters" "Groups and Options" tabs.

Click the Verifier tab.

Type the sample text in the Sample Input field.

Click Verify Expression.

EventLogCentral displays Expression Matched! if the sample text matches or Expression not Matched! if the sample text does not match in the Match Expression field.

Click Copy to match description or Copy to filter description hyperlinks.

EventLogCentral copies the text to Match for specific information / Filter specific information fields.

18 Type the Title, Header, Footer, and Description.
19 Crosscheck the Disk cost analysis details.
20 Crosscheck the Analysis parameters.
21 Click Generate.
Quick View

Quick View allows you to refine the result set. Quick View reports are not stored in the hard disk; you have to explicitly export those reports. Click the Export icon on the top strip to export the report. The exported reports can also be viewed in the Dashboard.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Queue (background processing), Enable publishing option, and Updated Status via RSS options will not available if you select Quick View as Export type.</td>
</tr>
</tbody>
</table>

Custom column analysis

1. Click On Demand in the Actions pane.
2. Click Next >>.
3. Select the Select custom properties option.
4. Type appropriately in the relevant fields.
5. Select the system(s) / group(s) / site(s).
6. Select the Format option as Detail.
7. Select the report generation Interval.
   EventLogCentral selects the Export Type as Excel.
8. Select the Custom column option.
   EventLogCentral displays the “Select or add Column(s) to display” page.

**DEFAULT**

Select the check boxes against the Column Name(s) to Add to Report.
You can also add custom columns. Click Add New Column to add custom columns.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Type the alias of the column in this field. This could be any name and it is mandatory. Accepts characters and numbers excluding special characters.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Column name</td>
<td>Type the name of the column in this field. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td>Add to selected columns</td>
<td>This is a shortcut to add the new columns to Selected Columns list. Type a column name and then click Add. EventLogCentral does not save the new column names into the database.</td>
</tr>
<tr>
<td>Save this column name</td>
<td>This is a shortcut to add the new columns to the Selected Columns list and EventLogCentral saves the new column names into the database. Type a column name and then click Add.</td>
</tr>
<tr>
<td>Columns in Report</td>
<td>EventLogCentral includes the columns that are selected in the report. You can also arrange the order of the columns that should appear in the report by selecting the columns and then by clicking the arrow keys.</td>
</tr>
<tr>
<td>Summary</td>
<td>Select the check boxes against the columns. These columns are included in the summary of the report. Event Description, Event Id, and Log Time cannot be included in the summary.</td>
</tr>
<tr>
<td>Sort by</td>
<td>Select an appropriate option of the sort order from this drop-down list.</td>
</tr>
</tbody>
</table>

EventLogCentral displays the selected columns in the **Columns in Report** field.

Set the order of the columns that you want to display in the report by selecting columns in **Columns in Report** and clicking arrow buttons.

Select the **Sort by** option and then click Next>>.

**ADVANCED**

Separator is a character that separates the key and its value. Terminator is a character that concludes the key.

Separator and Terminator feature facilitates you to query and highlight parts of clogged Syslog like messages, as columns in reports. Since there is no standardized message format and different conventions are being followed by vendors of NIX systems, it is difficult even for a seasoned user to decipher Syslog messages. Being said that, it is expected to have familiarity with Syslog message formats of different flavors of NIX systems.

By default, Windows separator is a colon (:) and terminator is a new line character (\n).
### Table 35

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Type the alias of the column in this field. This could be any name and it is mandatory. Accepts characters and numbers excluding special characters.</td>
</tr>
<tr>
<td>Column name</td>
<td>Type the name of the column in this field. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td>Add to selected</td>
<td>This is a shortcut to add the new columns to Selected Columns list. Enter a column name and then click Add. EventLogCentral does not save the new column names into the database.</td>
</tr>
<tr>
<td>columns</td>
<td></td>
</tr>
<tr>
<td>Separator</td>
<td>Type the separator character. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td>Terminator</td>
<td>Type the terminator character. Accepts any character and numbers including special characters.</td>
</tr>
<tr>
<td>Resolution</td>
<td>Resolution drop-down list is enabled only when the Advanced option is selected. This option helps to resolve IP address of the host by doing DNS lookup and view event &amp; port details in the EventTracker Knowledge Base. EventLogCentral adds hyperlinks in the generated report that enables you to navigate to the EventTracker Knowledge Base Web site to get more information on Events and ports and DNS lookup Web site to resolve IP address.</td>
</tr>
<tr>
<td>Columns in Report</td>
<td>EventLogCentral includes the columns that are selected in the report. You can also arrange the order of the columns that should appear in the report by selecting the columns and then by clicking the arrow keys.</td>
</tr>
<tr>
<td>Summary</td>
<td>Select the check boxes against the columns. These columns are included in the summary of the report. Event Description, Event Id, and Log Time cannot be included in the summary.</td>
</tr>
<tr>
<td>Sort by</td>
<td>Select an appropriate option of the sort order from this drop-down list.</td>
</tr>
</tbody>
</table>

### Table 36

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New Column</td>
<td>Add the column name to the Available Columns list. You have to explicitly click Add &gt; to add those columns to the Selected Columns list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add to selected columns</td>
<td>This is a shortcut to add the new columns to Selected Columns list. Type a column name and then click <strong>Add</strong>. EventLogCentral does not save the new column names into the database.</td>
</tr>
<tr>
<td>Save this column key</td>
<td>This is a shortcut to add the new columns to the Selected Columns list and EventLogCentral saves the new column names into the database. Type a column name and then click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

**Table 37**

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify</td>
<td>Select a row, select the check box at the right hand side and then click <strong>Modify</strong> to edit the selected row. EventLogCentral displays the Separator and Terminator fields. Modify appropriately and then click <strong>Update</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select a row, select the check box at the right hand side and then click <strong>Delete</strong> to delete the selected row.</td>
</tr>
</tbody>
</table>

Select the check boxes against the predefined **Column Name(s)** to **Add to Report**.
You can also add custom columns. Click **Add New Column** to add custom columns.
EventLogCentral displays the selected columns in the **Columns in Report** field.
Set the order of the columns that you want to display in the report by selecting columns in **Columns in Report** and clicking arrow buttons.
Select the **Sort by** option and then click **Next>>**.

9  Type the Refine and Filter criteria.
10 Type the Title, Header, Footer, and Description.
11 Crosscheck the Disk cost analysis details.
12 Crosscheck the Analysis parameters.
13 Click **Generate**.

**Note**

You can also select the **Add to queue** check box. EventLogCentral enables the **Enable publishing option** check box and **Update status via RSS** drop-down list. Select an appropriate publishing option.
You can also exclude predefined columns from the report. EventLogCentral does not save this exclusion in the database.

Log Analysis - Summary - On Demand

Standard column analysis

1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2. Click the Reports tab.
3. Click the Analysis option.
4. Click Logs in the Analysis tree.
5. Click On Demand in the Actions pane.
6. Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
7. Select the Select an event category option.
8. Select the Categories.
9. Click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.
10. Select the system(s) / group(s) / site(s).
    EventLogCentral displays the “Interval and More Options” page.
11. Select the Format option as Summary.
12. Select the report generation Interval.
13. Select the Export type as Quick View.
14. Select the Sort by option.
15. Type the Refine and Filter criteria.
16. Type the Title, Header, Footer, and Description.
17. Crosscheck the Disk cost analysis details.
18. Crosscheck the Analysis parameters.
19. Click Generate.
Quick View (Smart Viewer)

Smart Viewer allows you to subtly refine the intricate result set with ease. Initially Smart Viewer displays the Summary, Extended Summary and then the Detailed view. Presently supports On Demand Category based reports (Summary & Extended Summary) and Log Analysis (Summary) based on Event Categories and Custom Properties.

Note

Add to queue (background processing), Enable publishing option, and Updated status via RSS options will not available if you select Quick View as Export type.

- Click a record to view the Extended Summary.
Click a record to view details and refine the result set.

Click the hyperlink in the Event Id column to view the event details in EventTracker Knowledge Base.
Custom column analysis

1. Click **On Demand** in the Actions pane.
2. Click Next >>.
3. Select the **Select custom properties** option.
4. Type appropriately in the relevant fields.
5. Select the system(s) / group(s) / site(s).
6. Select the **Format option** as **Summary**.
7. Select the report generation Interval.
8. Select the Export type.

**Note**

Export type can be of any type and need not be Excel. Custom columns will be displayed as Row summary information and not as column in the report as done in the case of detail report.

9. Select the **Custom column** option.
   EventLogCentral displays the “Select or add Column(s) to display” page.
10. Add / Modify columns.
    EventLogCentral displays the selected columns in the **Columns in Report** field.
11. Set the order of the columns that you want to display in the report by selecting columns in **Columns in Report** and clicking arrow buttons.
12. Select the **Sort by** option and then click Next>>.
13. Type the Refine and Filter criteria.
14. Type the Title, Header, Footer, and Description.
15. Crosscheck the Disk cost analysis details.
16. Crosscheck the Analysis parameters.
17. Click **Generate**.
Note

You can also select the **Add to queue** check box. EventLogCentral enables the **Enable publishing option** check box and **Update status via RSS** drop-down list. Select an appropriate publishing option.

You can also exclude predefined columns from the report. EventLogCentral does not save this exclusion in the database.

---

**Log Analysis - Trend - On Demand**

**Standard / Custom column analysis**

1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2. Click the **Reports** tab.
3. Click the **Analysis** option.
4. Click **Logs** in the Analysis tree.
5. Click **On Demand** in the Actions pane.
   ELC displays the Reports Wizard.
6. Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
7. Select the **Select an event category** option.
8. Select the **Categories**.
   (OR)
   Select the **Select custom properties** option.
   Type appropriately in the relevant fields.
9. Click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.
10. Select the system(s) / group(s) / site(s).
    EventLogCentral displays the “Interval and More Options” page.
11. Select the **Format option** as **Trend**.
12 Select the report generation interval.

Select the interval for analysis:

Select this option, EventLogCentral considers events occurred during the selected number of days for analysis. Select this option and select Limit to time range check box. EventLogCentral enables the From and To spin boxes. Set the time range. EventLogCentral considers only events occurred in that time range for analysis.
Select custom date range:

Select this option, EventLogCentral considers events occurred during the selected number of days for analysis. Select this option and select Limit to time range check box. EventLogCentral enables the From and To spin boxes. Set the time range. EventLogCentral considers only events occurred in that time range for analysis.

Note that EventLogCentral considers only the date range from the From, To drop-down lists and ignores the time range set in those drop-down lists.

Figure 124 Limit to time range
Select the **Export type**.

Select the **Sort by** option.

Type the Refine and Filter criteria.

Type the Title, Header, Footer, and Description.
Log Analysis - Detail - Queued

Standard column analysis

1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2. Click the Reports tab.
3. Click the Analysis option.
4. Click Logs in the Analysis tree.
5. Click On Demand in the Actions pane.
6. Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
7. Select the Select an event category option.
8. Select the Categories.
9. Click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.
10. Select the system(s) / group(s) / site(s).
11. Select the Format option as Detail.
12. Select the report generation Interval
13. Select the Export type.
14. Select the Sort by option.
15. Type the Refine and Filter criteria.
16. Type the Title, Header, Footer, and Description.
17. Crosscheck the Disk cost analysis details.
18. Select the Add to queue check box.
19. Crosscheck the Analysis parameters.
20. Click Add To Queue.
Custom column analysis

1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2. Click the Reports tab.
3. Click the Analysis option.
4. Click Logs in the Analysis tree.
5. Click On Demand in the Actions pane.
6. Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
7. Select the Select custom properties option.
8. Type appropriately in the relevant fields.
9. Click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.
10. Select the system(s) / group(s) / site(s).
11. Select the Format option as Detail.
12. Select the report generation Interval.
13. Select the Export Type.
14. Select the Custom column option.
   EventLogCentral displays the “Select or add Column(s) to display” page.
15. Add / Modify columns.
   EventLogCentral displays the selected columns in the Columns in Report field.
16. Set the order of the columns that you want to display in the report by selecting columns in Columns in Report and clicking arrow buttons.
   EventLogCentral displays the selected columns in the Columns in Report field.
17. Select the Sort by option and then click Next>>.
18. Type the Refine and Filter criteria.
19. Type Title, Header, Footer, and Description.
20. Select the Add to queue check box.
22. Crosscheck the Analysis parameters.
23. Click Add To Queue.
(OR)
1 Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2 Click the **Reports** tab.
3 Click the **Analysis** option.
4 Click **Logs** in the Analysis tree.
5 Click **Queued** in the Actions pane.
6 Click **New** in the Queued pane.
7 Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
8 Set the rule and click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.
9 Click Next >>.
10 Select the system(s) / group(s) / site(s).
11 Select the **Format option** as **Detail**.
12 Select the report generation Interval.
13 Type the Refine and Filter criteria.
14 Type the Title, Header, Footer, and Description.
15 Crosscheck the Disk cost analysis details.
16 Crosscheck the Analysis parameters.
17 Click **Add To Queue**.

**Note**

Select the Enable publishing option check box and Update status via RSS drop-down list. Select an appropriate publishing option.

**Quick View** Export Type option is not available when you add a new analysis to queue by clicking Queued in the Actions pane.
Log Analysis - Summary - Queued

Standard column analysis

1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2. Click the Reports tab.
3. Click the Analysis option.
4. Click Logs in the Analysis tree.
5. Click On Demand in the Actions pane.
6. Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
7. Set the rule and click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.
8. Select the system(s) / group(s) / site(s).
9. Select the Format option as Summary.
10. Select the report generation Interval
11. Select the Export type.
12. Type the Refine and Filter criteria.
13. Type the Title, Header, Footer, and Description.
15. Select the Add to queue check box.
16. Crosscheck the Analysis parameters.
17. Click Add To Queue.
(OR)
1. Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2. Click the Reports tab.
3. Click the Analysis option.
4. Click Logs in the Analysis tree.
5. Click Queued in the Actions pane.
6. Click New in the Queued pane.
7. Click Next >>.
8 Set the rule and click Next >>.
9 Select the system(s) / group(s) / site(s).
10 Select the **Format option** as **Summary**.
11 Select the report generation Interval and Export type.
12 Type the Refine and Filter criteria.
13 Type the Title, Header, Footer, and Description.
14 Crosscheck the Disk cost analysis details.
15 Crosscheck the Analysis parameters.
16 Click **Add To Queue**.

**Note**

Select the **Add to queue** check box. EventLogCentral enables the **Enable publishing option** check box and **Update status via RSS** drop-down list. Select an appropriate publishing option.

**Quick View** Export Type option is not available when you add a new analysis to queue by clicking Queued in the Actions pane.

---

**Custom column analysis**

1 Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2 Click the **Reports** tab.
3 Click the **Analysis** option.
4 Click **Logs** in the Analysis tree.
5 Click **On Demand** in the Actions pane.
6 Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
7 Select the **Select custom properties** option.
8 Type appropriately in the relevant fields.
9 Click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.
10 Select the system(s) / group(s) / site(s).
11 Select the Format option as Summary.
12 Select the report generation Interval.
13 Select the Export type.

**Note**

Export type can be of any type and need not be Excel. Custom columns will be displayed as Row summary information and not as column in the report as done in the case of detail report.

14 Select the Custom column option.
   EventLogCentral displays the “Select or add Column(s) to display” page.
15 Add / Modify columns.
   EventLogCentral displays the selected columns in the Columns in Report field.
16 Set the order of the columns that you want to display in the report by selecting columns in **Columns in Report** and clicking arrow buttons.
17 Select the Sort by option and then click Next>>.
18 Type the Refine and Filter criteria.
19 Type Title, Header, Footer, and Description.
20 Crosscheck the Disk cost analysis details.
21 Select the Add to queue check box.
22 Crosscheck the Analysis parameters.
23 Click Add To Queue.

---

**Log Analysis - Trend - Queued**

**Standard column analysis**

1 Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2 Click the Reports tab.
3 Click the Analysis option.
4 Click Logs in the Analysis tree.
5 Click On Demand in the Actions pane.
6 Click Next >>.
EventLogCentral displays the “Select required category/properties of events to analyze” page.

7 Select the Select an event category option.

8 Select the Categories.

9 Click Next >>.
EventLogCentral displays the monitored Groups and Systems page.

10 Select the system(s) / group(s) / site(s).

11 Select the Format option as Trend.

12 Select the report generation interval.

Select the interval for analysis:
Select this option, EventLogCentral considers events occurred during the selected number of days for analysis. Select this option and select Limit to time range check box. EventLogCentral enables the From and To spin boxes. Set the time range. EventLogCentral considers only events occurred in that time range for analysis.

Select custom date range:
Select this option, EventLogCentral considers events occurred during the selected number of days for analysis. Select this option and select Limit to time range check box. EventLogCentral enables the From and To spin boxes. Set the time range. EventLogCentral considers only events occurred in that time range for analysis.

Note that EventLogCentral considers only the date range from the From, To drop-down lists and ignores the time range set in those drop-down lists.

13 Select the Export type.

14 Type the Refine and Filter criteria.

15 Type the Title, Header, Footer, and Description.

16 Crosscheck the Disk cost analysis details.

17 Select the Add to queue check box.

18 Crosscheck the Analysis parameters.

19 Click Add To Queue.

(OR)

1 Log on to EventLogCentral.
EventLogCentral displays the Home dashboard.

2 Click the Reports tab.

3 Click the Analysis option.
4 Click **Logs** in the Analysis tree.
5 Click **Queued** in the Actions pane.
6 Click **New** in the Queued pane.
7 Click Next >>.
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
8 Set the rule and click Next >>.
   EventLogCentral displays the monitored Groups and Systems page.
9 Click Next >>.
10 Select the system(s) / group(s) / site(s).
11 Select the **Format option** as **Trend**.
12 Select the report generation Interval.
13 Type the Refine and Filter criteria.
14 Type the Title, Header, Footer, and Description.
15 Crosscheck the Disk cost analysis details.
16 Crosscheck the Analysis parameters.
17 Click **Add To Queue**.

**Note**

Select the **Enable publishing option** check box and **Update status via RSS** drop-down list. Select an appropriate publishing option.

**Quick View** Export Type option is not available when you add new analysis to queue by clicking Queued in the Actions pane.

---

**Log Analysis - Detail - Scheduled**

**Standard column analysis**

1 Click the **Analysis** option.
2 Click **Logs** in the Analysis tree.
3 Click **Scheduled** in the Actions pane.
4 Click **New** in the Scheduled pane.
5 Click Next >>.
EventLogCentral displays the “Select required category/properties of events to analyze” page.

6 Select the **Select an event category** option.

7 Click Next>>.

8 Select the system(s) / group(s) / site(s).

9 Select the **Format option** as **Detail**.

10 Select the Schedule interval.

**Note**

Select the Schedule interval. If you select the Schedule Type as Daily / Weekly, then EventLogCentral displays the **Limit to time range** check box. Set the time range. EventLogCentral considers only events occurred in that specified time range.

11 Select the Export type.

12 Type the Refine and Filter criteria.

13 Type the Title, Header, Footer, and Description.

14 Crosscheck the Disk cost analysis details.

15 Select the **Enable publishing option** check box to deliver or notify results via E-mail. Type valid **To E-mail** address.

16 Select RSS Feed from the **Update status via RSS** to receive RSS notification.

17 Crosscheck the Analysis parameters.

18 Click **Schedule**.

---

**Custom column analysis**

1 Click the **Analysis** option.

2 Click **Logs** in the Analysis tree.

3 Click **Scheduled** in the Actions pane.

4 Click **New** in the Scheduled pane.

5 Click Next >>.

EventLogCentral displays the “Select required category/properties of events to analyze” page.
Select the **Select custom properties** option.

Select the system(s) / group(s) / site(s).

Select the **Format option** as **Detail**.

Select the Schedule interval.

**Note**

Select the Schedule interval. If you select the Schedule Type as Daily / Weekly, then EventLogCentral displays the **Limit to time range** check box. Set the time range. EventLogCentral considers only events occurred in that specified time range.

Select the **Custom column analysis** option. EventLogCentral selects the Export Type Excel.

Click Next>>.

EventLogCentral displays the “Select or add Column(s) to display” page.

Add / Modify columns.

EventLogCentral displays the selected columns in the Columns in Report field.

Set the order of the columns that you want to display in the report by selecting columns in **Columns in Report** and clicking arrow buttons.

Select the **Sort by** option and then click Next>>.

Type the Refine and Filter criteria.

Type the Title, Header, Footer, and Description.

Crosscheck the Disk cost analysis details.

Select the **Enable publishing option** check box to deliver or notify results via E-mail. Type valid **To E-mail** address.

Select RSS Feed from the **Update status via RSS** to receive RSS notification.

Crosscheck the Analysis parameters.

Click **Schedule**.

**Note**

**Quick View** Export Type option is not available when you schedule an analysis.
EventLogCentral enables **Week Day** drop-down list only when you select the **Weekly** option from the **Schedule Type** drop-down list.

---

**Log Analysis - Summary - Scheduled**

**Standard column analysis**

1. Click the **Analysis** option.
2. Click **Logs** in the Analysis tree.
3. Click **Scheduled** in the Actions pane.
4. Click **New** in the Scheduled pane.
5. Click Next >>.

   EventLogCentral displays the “Select required category/properties of events to analyze” page.

6. Select the **Select an event category** option.
7. Click Next >>.
8. Select the system(s) / group(s) / site(s).
9. Select the **Format option** as **Summary**.
10. Select the Schedule interval.

**Note**

Select the Schedule interval. If you select the Schedule Type as Daily / Weekly, then EventLogCentral displays the **Limit to time range** check box. Set the time range. EventLogCentral considers only events occurred in that specified time range.

11. Select the Export type.
12. Type the Refine and Filter criteria.
13. Type the Title, Header, Footer, and Description.
15. Select the **Enable publishing option** check box to deliver or notify results via E-mail. Type valid **To E-mail** address.
16 Select RSS Feed from the Update status via RSS to receive RSS notification.

17 Crosscheck the Analysis details.

18 Click Schedule.

---

**Custom column analysis**

1 Click the Analysis option.

2 Click Logs in the Analysis tree.

3 Click Scheduled in the Actions pane.

4 Click New in the Scheduled pane.

5 Click Next >>.

EventLogCentral displays the “Select required category/properties of events to analyze” page.

6 Select the Select custom properties option.

7 Type appropriately in the relevant fields.

8 Click Next >>.

9 Select the system(s) / group(s) / site(s).

10 Select the Format option as Summary.

11 Select the Custom Column option.

12 Select the Schedule interval.

---

**Note**

Select the Schedule interval. If you select the Schedule Type as Daily / Weekly, then EventLogCentral displays the Limit to time range check box. Set the time range. EventLogCentral considers only events occurred in that specified time range.

13 Click Next>>.

EventLogCentral displays the “Select or add Column(s) to display” page.

14 Add / Modify columns.

EventLogCentral displays the selected columns in the Columns in Report field.

15 Set the order of the columns that you want to display in the report by selecting columns in Columns in Report and clicking arrow buttons.

16 Select the Sort by option and then click Next>>.
17 Select the Export Type.

**Note**

Export type can be anything and need not be Excel. Custom columns will be displayed as Row summary information and not as column in the report as done in the case of detail report.

18 Type the Refine and Filter criteria.
19 Type the Title, Header, Footer, and Description.
20 Crosscheck the Disk cost analysis details.
21 Select the **Enable publishing option** check box to deliver or notify results via E-mail. Type valid **To E-mail** address.
22 Select RSS Feed from the **Update status via RSS** to receive RSS notification.
23 Crosscheck the Analysis details.
24 Click **Schedule**.

---

**Log Analysis - Trend - Scheduled**

**Standard column analysis**

1 Click the **Analysis** option.
2 Click **Logs** in the Analysis tree.
3 Click **Scheduled** in the Actions pane.
4 Click **New** in the Scheduled pane.
5 Click Next >>.
   
   EventLogCentral displays the “Select required category/properties of events to analyze” page.
6 Select the **Select an event category** option.
7 Click Next>>.
8 Select the system(s) / group(s) / site(s).
9 Select the **Format option** as **Trend**.
10 Select the Schedule interval.
Select the Schedule interval. If you select the Schedule Type as Daily / Weekly, then EventLogCentral displays the Limit to time range check box. Set the time range. EventLogCentral considers only events occurred in that specified time range.

11 Select the Export type.
12 Type the Refine and Filter criteria.
13 Type the Title, Header, Footer, and Description.
14 Crosscheck the Disk cost analysis details.
15 Select the Enable publishing option check box to deliver or notify results via E-mail. Type valid To E-mail address.
16 Select RSS Feed from the Update status via RSS to get RSS notification.
17 Crosscheck the Analysis details.
18 Click Schedule.

Quick View Export Type option is not available when you schedule a new analysis.

EventLogCentral enables Week Day drop-down list only when you select the Weekly option from the Schedule Type drop-down list.

**Log Analysis - Detail - Defined**

**Standard column analysis**

1 Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2 Click the Reports tab.
3 Click the Analysis option.
4 Click Logs in the Analysis tree.
5 Click Defined in the Actions pane.
Click **New**. EventLogCentral displays the Reports Wizard.

Click Next >>. EventLogCentral displays the “Select required category/properties of events to analyze” page.

Select the **Select an event category** option.

Select the **Categories**.

Click Next >>. EventLogCentral displays the monitored Groups and Systems page.

Select the system(s) / group(s) / site(s).

EventLogCentral displays the “Interval and More Options” page. Interval option is disabled for Defined Log Analyses.

**Figure 127 Defined Detail Log Analysis**

**12** Select the **Format option** as **Detail**.

**13** Select the **Export type**.

**14** Select the **Sort by** option.

**15** Type the Refine and Filter criteria.

**16** Type the Title, Header, Footer, and Description.

**17** Crosscheck the Disk cost analysis details.

**18** Crosscheck the Analysis parameters.
Custom column analysis

1. Click On Demand in the Actions pane.
2. Click Next >>.
3. Select the Select custom properties option.
4. Type appropriately in the relevant fields.
5. Select the system(s) / group(s) / site(s).
6. Select the Format option as Detail.
7. Select the report generation Interval.
8. Select the Export Type.
9. Select the Custom column option.
   EventLogCentral displays the “Select or add Column(s) to display” page.
   EventLogCentral displays the selected columns in the Columns in Report field.
10. Set the order of the columns that you want to display in the report by selecting columns in Columns in Report and clicking arrow buttons.
11. Select the Sort by option and then click Next>>.
12 Type the Refine and Filter criteria.
13 Type the Title, Header, Footer, and Description.
14 Crosscheck the Disk cost analysis details.
15 Crosscheck the Analysis parameters.
16 Click Save.

---

**Resolving IP Address and viewing Event ID, Port details**

This option helps to resolve IP address by DNS Lookup and view event and port details in the EventTracker Knowledge Base web site.

**Viewing port details in EventTracker KB**

To view port details in EventTracker KB

1 Log on to EventLogCentral.
2 Click the **Reports** tab.
3 Click the **Analysis** tab.
4 Under Logs, click **Detail**.
5 Select **On Demand** from the shortcut menu.
6 Select the **Select Custom properties** option.
7 Enter/type appropriately in the relevant fields. Example: Event ID 3225
8 Select the systems.
9 Set the Interval.
10 Select the **Custom column** option.
   Export Type: Excel Document (*.xls) is selected by default.
11 Select the **Advanced** option.
12 Click **Add New Column** to add custom columns. **Resolution** drop-down list is enabled only when the “Advanced” option is selected.
13 Enter/select the custom column details as shown below.

14 Click Add.

EventLogCentral adds the custom column as shown below.
Similarly add “Remote Port” custom column.

Select the columns in the “Selected Items” list and then up and down arrow button to arrange the column order that should appear in the generated report.

Select the Sort by option.

Set the Search criteria.

Type appropriate analysis title, description, header and footer.

Crosscheck Analysis cost details.

Crosscheck Analysis configuration summary.

Click Generate.

EventLogCentral displays the pop-up window.
23 Click **Open** to view the generated report.

24 Click the hyperlinks in the Local Port and Remote Port columns. EventLogCentral moves you to the EventTracker Knowledge Base Web site.
Resolving IP address

Generate an analysis with custom columns “Source IP” and “Destination IP”
Click the hyperlinks in the Source IP and Destination IP columns. Advanced Reports moves you through the Whois Lookup Web site.
Viewing generated Queued Log Analysis

To view generated Queued Log Analysis

1. Click **Queued** in the Actions pane.
2. Click the links in the **Title** column to view the reports.
   EventLogCentral displays the File Download pop-up window.
3. Click **Open** to view the report.
   EventLogCentral displays the generated report.

   **Note**
   Click to refresh the top pane.

Searching generated Queued Log Analysis

To search generated Queued Log Analysis

1. Click **EventLogCentral** displays the Search page.
   By default, EventLogCentral searches reports that are generated in the past 24 hours. So, select the date appropriately from the Calendar control if you are not sure about the date.
2. Type appropriate details in the relevant fields.
3. Click **Search**.
   EventLogCentral displays the search result.
4. Click **Show All** to view all the generated reports.

Exporting summary report on generated Log Analysis

To export summary report

1. Click **EventLogCentral**
EventLogCentral displays the File Download pop up.

2 Click **Open** to view the report or **Save** to save the report in the hard disk.

---

### Log Analysis Report queue statistics

To view Log Analysis Report queue statistics

- Click the **Queued** link in the Actions pane.
  
  EventLogCentral displays the statistics in the bottom pane.

---

### Log Analysis queue statistics - Admin

To view Log Analysis queue statistics

1 Log in as user with Admin Privilege.

2 Click the **Queued** in the Actions pane.
  
  EventLogCentral displays the statistics in the bottom pane.

3 Click **Show All User Reports**.
  
  ELC displays the Log Analysis Report Queue Statistics pane.

4 Click **Show Reports Configured By Me** to view the reports configured by you.

---

### Alert Analysis

EventTracker includes a category or group of event logs called ***Alerts***. Those logs that require immediate attention are included in this group.

Alert Analysis shows event logs of this category.

Usage: Quickly review recent critical event logs.

---

### Alert Analysis - On Demand

1 Log on to EventLogCentral.
  
  EventLogCentral displays the Home dashboard.
2 Click the Reports tab.
3 Click the Analysis option.
   EventLogCentral displays the Analysis page.
4 Click Alerts in the Analysis tree.
   EventLogCentral displays the Alerts Dashboard.
5 Click On Demand in the Actions pane.
6 Click Next >>.
7 Select the System(s) / Group(s) / Site(s).
8 Select the report generation Interval, Format option and Export type.
9 Type the Refine and Filter criteria. You can skip this step, if you do not have any criteria to set.
10 Type the Title, Header, Footer, and Description.
11 Crosscheck the Analysis cost details.
12 Crosscheck the Analysis details.
13 Click Generate.

Quick View

Quick View allows you to refine the result set. Quick View reports are not stored in the hard disk; you have to explicitly export those reports. Click the Export icon on the top strip to export the report. The exported reports can also be viewed in the Dashboard.

**Note**

You can also select the Add to queue check box. EventLogCentral enables the Enable publishing option check box. Select an appropriate publishing option.

You can also link a RSS Feed to the report.

Alert Analysis - Queued

1 Click the Analysis option.
2 Click Alerts in the Analysis tree.
3 Click On Demand in the Actions pane.
4. Click Next >>.
5. Select the System(s) / Group(s) / Site(s).
7. Type the Refine and Filter criteria.
8. Type the Title, Description, Footer, and Description.
10. Select the Add to queue check box.
11. Crosscheck the Analysis details.
12. Click Add To Queue.

(OR)

1. Click the Analysis option.
2. Click Alerts in the Analysis tree.
3. Click Queued in the Actions pane.
4. Click New in the Queued pane.
5. Click Next >>.
6. Select the System(s) / Group(s) / Site(s).
7. Select the report generation Interval, Format option and Export type.
8. Type the Refine and Filter criteria.
9. Type the Title, Description, Footer, and Description.
10. Crosscheck the Analysis cost details.
11. Crosscheck the Analysis details.
12. Click Add To Queue.

**Note**

Quick View Export Type option is not available when you add a new analysis to queue.

---

**Alert Analysis - Scheduled**

1. Click the Analysis option.
2. Click Alerts in the Analysis tree.
3. Click Scheduled in the Actions pane.
4 Click **New** in the Scheduled pane.
5 Click Next >>.
6 Select the System(s) / Group(s) / Site(s).
7 Select the **Schedule interval**, **Format option** and **Export Type**.
8 Type the Refine and Filter criteria.
9 Type the Title, Header, Footer, and Description.
10 Crosscheck Analysis cost details.
11 Crosscheck the Analysis details.
12 Select the **Enable publishing option** check box.
13 Click **Schedule**.

**Note**

*Quick View* Export Type option is not available when you schedule an analysis.

EventLogCentral enables **Week Day** drop-down list only when you select the **Weekly** option from the **Schedule Type** drop-down list.

---

**Tracking Alert Notification Status**

This report helps to track the success/failure status of the configured Alert Actions (Beep, E-mail, Message, Forward, and Custom).

To track Alert Notification status
1 Click **Reports** tab.
2 Click **Advanced** or **My Reports** option.
3 Click the **Operations** tab.
4 Expand the **Alerts** report group.
5 Select the **Alert Notification** Report.
6 Click **Queued / On Demand Report** in the Actions pane.
7 Click **New On Demand** in the Queued pane.
8 Click Next >>.
9 Select the **Categories** for which you have configured Alert Actions.
10 Click Add >>.
11 Select action type(s) you have set.
12 Click Next >>.
13 Select the report generation Interval and Export type.
14 Type the Title, Header Footer, and Description.
15 Crosscheck the Report cost details.
16 Crosscheck the Report details.
17 Click Generate.

**Note**
You can also Queue, Schedule and Define this report.

---

**Log Volume Analysis**

Filter and display event logs based on user defined criteria. The user can define he filter (or exclude) string as well as specify the output format.

Usage: Forensic Analysis of specific events, broad searches per criteria with subsequent sorting and ordering of the result set.

---

**Log Volume Analysis - On Demand**

**Event Categories**

1 Log on to EventLogCentral.
   EventLogCentral displays the Home dashboard.
2 Click the Reports tab.
3 Click the Analysis option.
   EventLogCentral displays the “Analysis” page.
4 Click Log Volume in the Analysis tree.
5 Click On Demand in the Actions pane.
6 Click Next >>.
7 Select the Analyze events based on Event Categories option.
8 Select a category from **Category** drop-down list.
9 Select the System(s) / Group(s) / Site(s).
10 Select the report generation **Interval** and **Export type**.
11 Type the Refine and Filter criteria.
12 Type the Title, Header Footer, and Description.
13 Crosscheck the Analysis cost details.
14 Crosscheck the Analysis details.
15 Click **Generate**.

---

**Custom properties**

1 Click the **Analysis** option.
2 Click **Log Volume** in the Analysis tree.
3 Click **On Demand** in the Actions pane.
4 Click Next >>.
5 Select the **Analyze events based on Custom Properties** option.
6 Enter appropriately in the relevant fields.
7 Select the System(s) / Group(s) / Site(s).
8 Select the report generation **Interval** and **Export type**.
9 Type the Refine and Filter criteria.
10 Type the Title, Header, Footer, and Description.
11 Crosscheck the Analysis cost details.
12 Crosscheck the Analysis details.
13 Click **Generate**.

---

**Event Id**

1 Click the **Analysis** option.
2 Click **Log Volume** in the Analysis tree.
3 Click **On Demand** in the Actions pane.
4 Click Next >>.
5 Select the **Analyze events based on Event Id** option.
6 Select Event Id(s).
7 Select Display all records or Display only top "n" records option.
8 Select the System(s) / Group(s) / Site(s).
9 Select the report generation Interval and Export type.
10 Type the Refine and Filter criteria.
11 Type the Title, Header, Footer, and Description.
12 Crosscheck the Analysis cost details.
13 Crosscheck the Analysis details.
14 Click Generate.

Note

You can also select the Add to queue check box. EventLogCentral enables the Enable publishing option check box. Select an appropriate publishing option.

Log Volume Analysis - Queued
1 Click the Analysis option.
2 Click Log Volume in the Analysis tree.
3 Click On Demand in the Actions pane.
4 Click Next >.
5 Select the Analyze events based on Event categories/Custom properties/Event Id option.
6 Select/enter appropriately.
7 Select the System(s) / Group(s) / Site(s).
8 Select the report generation Interval and Export type.
9 Type the Refine and Filter criteria.
10 Type the Title, Header, Footer, and Description.
11 Crosscheck Analysis cost details.
12 Select the Add to queue check box.
13 Crosscheck the Analysis details.
14 Click Add To Queue.

(OR)
1 Click the Analysis option.
2 Click Log Volume in the Analysis tree.
3 Click Queued in the Actions pane.
4 Click New in the Queued pane.
5 Click Next >>.
6 Select the Analyze events based on Event categories/Custom properties/Event Id option.
7 Select/enter appropriately.
8 Select the System(s) / Group(s) / Site(s).
9 Select the report generation Interval and Export type.
10 Type the Refine and Filter criteria.
11 Type the Title, Header, Footer, and Description.
12 Crosscheck the Analysis cost details.
13 Crosscheck the Analysis details.
14 Click Add To Queue.

Note

You can also select the Enable publishing option check box to deliver or notify results via E-mail. Type valid To E-mail address. Select RSS Feed from the Update status via RSS to get RSS notification.

Quick View Export Type option is not available when you schedule a new analysis.

Log Volume Analysis - Scheduled
1 Click the Analysis option.
2 Click Log Volume in the Analysis tree.
3 Click Scheduled in the Actions pane.
4 Click New in the Scheduled pane.
5 Click Next >>.
6 Select the Analyze events based on Event categories/Custom properties/Event Id option.
7 Select/enter appropriately.
8 Select the System(s) / Group(s) / Site(s).
9 Select the report generation Interval and Export type.
10 Type the Refine and Filter criteria.
11 Type the Title, Header, Footer, and Description.
12 Crosscheck the Analysis cost details.
13 Crosscheck the Analysis details.
14 Click Schedule.

**Note**

You can also select the **Enable publishing option** check box to deliver or notify results via E-mail. Type valid **To E-mail** address. Select RSS Feed from the **Update status via RSS** to get RSS notification.

**Quick View** Export Type option is not available when you schedule a new analysis.

EventLogCentral enables **Week Day** drop-down list only when you select **Weekly** as Schedule Type.

---

**Suspicious Traffic Analysis**

The classic virus infection causes unrecognized EXEs to begin accessing the network. When enabled, the EventTracker Agent for Windows can be configured with a white-list of known ports or application and report exceptions. This helps identify potentially suspicious traffic. The report uses a database of known infections per port to identify potential threats.

Usage: After suitably configuring the EventTracker Agent for Windows, this report is used to report on unusual traffic from unrecognized EXEs.

- Select Suspicious Traffic Only (SNAM) option in Agent Configuration window under Network Connection Monitor tab prior to generating Suspicious Traffic Analysis reports.
- To receive alerts on the occurrence of suspicious traffic, select Suspicious Network Activity Alerts option in the Manager Configuration window.
Suspicious Traffic Analysis - On Demand

1. Click the Analysis option.
2. Click Suspicious Traffic in the Analysis tree.
3. Click On Demand in the Actions pane.
4. Click Next >>.
5. Select the System(s) / Group(s) / Site(s).
6. Select the report generation Interval and Export type.
7. Type the Refine and Filter criteria.
8. Type the Title, Header, Footer, and Description.
9. Crosscheck the Analysis cost details.
10. Crosscheck the Analysis details.
11. Click Generate.

Note

You can also select the Add to queue check box. EventLogCentral enables the Enable publishing option check box. Select an appropriate publishing option.

Suspicious Traffic Analysis - Queued

1. Click the Analysis option.
2. Click Suspicious Traffic in the Analysis tree.
3. Click On Demand in the Actions pane.
4. Click Next >>.
5. Select the System(s) / Group(s) / Site(s).
6. Select the report generation Interval and Export type.
7. Type the Refine and Filter criteria.
8. Type the Title, Header, Footer, and Description.
10. Select the Add to queue check box.
11. Crosscheck the Analysis details.
12. Click Add To Queue.
(OR)

1. Click the **Analysis** option.
2. Click **Suspicious Traffic** in the Analysis type.
3. Click **Queued** in the Actions pane.
4. Click **New** in the Queued pane.
5. Click Next >>.
6. Select the System(s) / Group(s) / Site(s).
7. Select the report generation Interval and Export type.
8. Type the Refine and Filter criteria.
9. Type the Title, Header, Footer, and Description.
10. Crosscheck the Analysis cost details.
11. Crosscheck the Analysis details.
12. Click **Add To Queue**.

**Note**

You can also select the **Enable publishing option** check box to deliver or notify results via E-mail. Type valid To E-mail address. Select RSS Feed from the **Update status via RSS** to get RSS notification.

**Quick View** Export Type option is not available when add new analysis to queue by clicking Queued in the Actions pane.

---

**Suspicious Traffic Analysis - Scheduled**

1. Click the **Analysis** option.
2. Click **Suspicious Traffic** in the Analysis tree.
3. Click **Scheduled** in the Actions pane.
4. Click **New** in the Scheduled pane.
5. Click Next >>.
6. Select the System(s) / Group(s) / Site(s).
7. Select the report generation **Interval** and **Export type**.
8. Type the Refine and Filter criteria.
9. Type the Title, Header, Footer, and Description.
10 Crosscheck the Analysis cost details.
11 Crosscheck the Analysis details.
12 Click Schedule.

Note

You can also select the Enable publishing option check box to deliver or notify results via E-mail. Type valid To E-mail address. Select RSS Feed from the Update status via RSS to get RSS notification.

Quick View Export Type option is not available when you schedule a analysis.

EventLogCentral enables Week Day drop-down list only when you select the Weekly as Schedule Type.

---

Cost Saving Analysis

EventTracker collects statistics of logs received, alerts issued, reports generated, system and service downtime etc. User defined variables such as time saved by process automation and labor hour cost information is used to compute cost and time savings accrued.

---

Person Hour

Time (in seconds) taken for manual analysis - The time required to perform each function manually. When automated by EventTracker, this is the time saved. These values are used to compute overall time/cost savings.

Labor rates (per hour) - Shows the fully loaded labor cost per hour of a system administrator's time. These values are use to compute total cost savings.

This option helps you generate On Demand reports in the foreground. You can also Queue or Schedule Person Hour Analysis.

---

On Demand
1 Click the Analysis option.
2 Click Cost Savings in the Analysis tree.
3 Click On Demand in the Actions pane.
Click Next >>.

Select the Interval, Format option, Export type, and Chart type.

Type the Title, Header, Footer, and Description.

Crosscheck the Analysis details.

Click Generate.

Queued
1 Click the Analysis option.
2 Click Cost Savings in the Analysis tree.
3 Click Queued in the Actions pane.
4 Click New in the Queued pane.
5 Click Next >>.
6 Select the Interval, Format option, Export type, and Chart type.
7 Type the Title, Header, Footer, and Description.
8 Select the Enable publishing option check box.
9 Select the Deliver results via E-mail option to deliver the report to the specified receiver mail id(s).
10 Select the Notify results via E-mail option to notify the report generation alone to the specified receiver mail id(s).
11 Select a RSS feed from the Update status via RSS drop-down list to receive RSS Alert notification.
12 Crosscheck the Analysis details.
13 Click Add to queue.

Scheduled
1 Click the Analysis option.
2 Click Cost Savings in the Analysis tree.
3 Click Scheduled in the Actions pane.
4 Click New in the Scheduled pane.
5 Click Next >>.
6 Select the Schedule type and Schedule time.
7 Select the Format option, Export type, and Chart type.
8 Type the Title, Header, Footer, and Description.
9 Select the Enable publishing option check box.
10 Select the Deliver results via E-mail option to deliver the report to the specified receiver mail id(s).
11 Select the **Notify results via E-mail** option to notify the report generation alone to the specified receiver mail id(s).

12 Select a RSS feed from the **Update status via RSS** drop-down list to receive RSS Alert notification.

13 Crosscheck the Analysis details.

14 Click **Schedule**.

**Note**

Quick View Export Type option is not available when you schedule/queue an analysis.

EventLogCentral enables **Week Day** drop-down list only when you select the **Weekly** as **Schedule Type**.
Chapter 6
Monitoring Enterprise Activities

In this chapter, you will learn how to:

- Analyze Enterprise Activity Volume
- Analyze per System Alerts
- Analyze non-Admin User Activities
- Analyze Admin User Activities
- Analyze Activities per System
- Analyze Events by Occurrences
- Analyze IP Addresses by Traffic
- Analyze Processes by Occurrence
- Configure Enterprise Activity
- Configure Filters
- Track Enterprise Activity Events
Monitoring Enterprise Activities

Enterprise Activity module helps you effectively monitor and manage enterprise activities.

It presents statistical data on:

- Alert events occurred.
- Admin & non-Admin user activities.
- Processes executed. Provision to get more information on processes.
- Activities occurred at a particular system/IP address. Provision to resolve IP addresses.
- Event IDs on occurrences. Provision to get more information on Event IDs.

Enterprise Activity Summary page presents consolidated tabular data and itemized graphical charts of monitored entities. Also facilitates to analyze Alerts through EventTracker Log Search browser and do Enterprise Activity Volume analysis.

Enterprise Activity Detail page presents details of the Enterprise Activities.

How it works

As the EventTracker Console receives events from monitored systems, it forwards those that relate to enterprise activities to the Correlation Engine. A ruleset at this correlation engine determines the event combinations that signal enterprise activities and presents the consolidated data in a comprehensible way.

Enterprise Activity Dashboard

This option helps to view summary of Enterprise Activities.

To view summary of Enterprise Activities
1. Log on to EventLogCentral.
2. Click the Enterprise Activity tab.

EventLogCentral displays the “Enterprise Activity Summary” page.
Click a pie on the chart or a legend to view respective activity details.

**Note**

By default, EventLogCentral displays 24-hour enterprise activities

### Analyzing Enterprise Activity Volume

This option helps to analyze enterprise activity log volume.

To analyze enterprise activity volume
Field | Description
---|---
Unique | Count of unique Event IDs.
Total Count | Total count of activities with respect to unique Event IDs.

1. Click the “Alerts” hyperlink to do per system Alert analysis.
2. Click any of the entities other than Alerts.

EventLogCentral displays the “Enterprise Activity Volume Analysis” window.
Select appropriately in the relevant fields and then click **Start**.
EventLogCentral displays respective consolidated list of activities.
4 Click the Print hyperlink to print the report.

Analyzing per System Alerts

The option helps to analyze Alert events occurred at the monitored systems.

To analyze Alerts

- Click a pie on the chart or a legend to view Alert details of the monitored systems.
(OR)

Click the **Alerts** hyperlink in the Enterprise Activity Volume Analysis pane.

<table>
<thead>
<tr>
<th></th>
<th>Unique</th>
<th>Total Count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alerts</strong></td>
<td>3</td>
<td>641</td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>13</td>
<td>482</td>
</tr>
<tr>
<td><strong>Admins</strong></td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td><strong>Event IDs</strong></td>
<td>138</td>
<td>692,876</td>
</tr>
<tr>
<td><strong>IPs</strong></td>
<td>20</td>
<td>467</td>
</tr>
<tr>
<td><strong>Processes</strong></td>
<td>113</td>
<td>2,522</td>
</tr>
<tr>
<td><strong>Systems</strong></td>
<td>3</td>
<td>692,876</td>
</tr>
</tbody>
</table>

**Note**

Move the mouse pointer over the chart or legend to view tooltip.

EventLogCentral displays the “Alert Analysis” page.
Analyzing non-Admin User Activities

This option helps you analyze non-admin user activities.

To analyze non-admin user activities

Following are the Event IDs considered for analyzing non-admin user activities.

<table>
<thead>
<tr>
<th>Non-VISTA SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 551, 642, 644, 647, 672, 675, 682, and 683.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VISTA SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624, 4625, 4634, 4647, 4738, 4740, 4768, 4771, 4778, and 4779.</td>
</tr>
</tbody>
</table>

User name and domain information is extracted from the Event Properties. If the user name and domain information is not proper in the Event Properties, it is extracted from the Event Description. For example, if the user name is either ‘LOCAL SERVICE’ or ‘ANONYMOUS LOGON’ or ‘N/A’ or ‘NETWORK SERVICE’ or ‘SYSTEM’ or contains ‘$’ or contains ‘IUSR’ then the proper user name is extracted from the Event Description.

Also, if the domain name is either ‘NT AUTHORITY’ or ‘N/A’ then the proper domain name is extracted from the Event Description.
1 Click a pie on the chart or a legend to view non-admin user activity details.

EventLogCentral displays the “Enterprise Activity Detail” page.
Figure 146 Users by Activity

Click | To
--- | ---
🔍 | Zoom a graph.
📊 | View Stacked Bar graph.
📊 | View Bar graph.
📊 | View Pie graph.
🗹 | Collapse a pane.
🗹 | Expand a pane.
🗹 | Collapse a pane.
🗹 | Expand a pane.
🔍 | Refresh the page.
🔍 | Search the search phrase.
Under Users tab, sort option, alphabetical list of users, search option, count of unique users monitored, and total count of non-admin user activities are displayed.

Panels on the right-hand side display non-admin user activity details.

2. Click the button to refresh the page with latest events.

First pane consists of two parts, first displays the activity details and the second displays the Weekly trend of activities.

<table>
<thead>
<tr>
<th>Event Id</th>
<th>Count</th>
<th>Sample Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S40</td>
<td>72</td>
<td>Successful Network Logon:</td>
</tr>
<tr>
<td>S38</td>
<td>71</td>
<td>User Logoff:</td>
</tr>
</tbody>
</table>

Second pane displays top 5 users by activities. Options are provided to select number of users and chart type to view.

Third pane displays out of ordinary user activities, helps to monitor abnormal user activities.
### Field | Description
--- | ---
**Total Count** | Total count of activities occurred during last 24 hours is displayed under this column.
**Average Count** | Average Count = Total count of activities / No. of days. Suppose the average count is taken on the 10th day, total count of activities occurred in the past 9 days divided by 9 days gives you the Average Count.
**Variation (%)** | 1. Positive Variation (when TotalCount - AvgCount = Positive)  
Variation% = ((TotalCount - AvgCount) / AvgCount) * 100  
2. Negative Variation (when TotalCount - AvgCount = Negative)  
Variation% = ((TotalCount - AvgCount) / TotalCount) * 100  
If the positive variation is greater than the Behavior correlation threshold and the negative correlation is less than the negative of Behavior correlation threshold, then the activity is considered as out-of-ordinary activity.

Fourth pane displays new user activities. Users are considered “New” based on “Behavior learning period”.

If the activities after the Behavior learning period do not intersect with the activities during the Behavior learning period, then that user is considered as a “New” user.

For example, the user activities occurred in the last 24 hours after the Behavior learning period is displayed in the New Users pane. Similarly the user activities occurred in the last 48 hours and 72 hours after the Behavior learning period is displayed in the New Users pane. For this, you have to set “Last 2 days” or “Last 3 days” option respectively as Generation Interval.

#### Click a hyperlink in the alphabetical list.
Type the search phrase in the search field and then click **Search**. EventLogCentral displays the list of users searched for.

4. To do a **Log Search**, select a row under the Users tab or a row in the first, third, and fourth panes.

EventLogCentral displays the drop-down list. From the drop-down list, choose **Log Search**.

EventLogCentral opens the Log Search browser with query results.
To view event details in the EventTracker Knowledge Base, select an event id under Event Id column in the first pane.

EventLogCentral displays the drop-down list.

From the drop-down list, choose Knowledge Base.

EventLogCentral displays the event details in the EventTracker Knowledge Base.
Click the Summary hyperlink to go back to the “Enterprise Activity Summary” page.

Analyzing Admin User Activities

This option helps you analyze admin user activities.

To analyze admin user activities

Following are the Event IDs considered for analyzing admin user activities.

<table>
<thead>
<tr>
<th>Table 42</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Non-VISTA SYSTEMS</strong></td>
</tr>
</tbody>
</table>

| **VISTA SYSTEMS** |
User name and domain information is picked up from the Event Properties. If the user name and domain information is not proper in the Event Properties, it is extracted from the Event Description. For example, if the user name is either 'LOCAL SERVICE' or 'ANONYMOUS LOGON' or 'N/A' or 'NETWORK SERVICE' or 'SYSTEM' or contains '$' or contains 'IUSR' then the proper user name is extracted from the Event Description.

Also, if the domain name is either 'NT AUTHORITY' or 'N/A' then the proper domain name is extracted from the Event Description.

1. Click a pie on the chart or a legend to view admin user activity details.

EventLogCentral displays the “Enterprise Activity Detail” page.
Under Admins tab, sort option, alphabetical list of admin users, search option, total number of admin users monitored, and total number of admin user activities are displayed.

Panels on the right-hand side display user activity details.

1. Click the refresh button to refresh the page with latest events.

First pane consists of two parts: first displays the event details and the second displays the Weekly trend of admin user activities.

Second pane displays top 5 users by activities. Options are provided to select number of admin users and chart type to view.

Third pane displays out of ordinary user activities. Helps to monitor abnormal user activities and it depends on the “Behavior correlation” criteria you set through the Configuration dialog box.

Fourth pane displays new user activities. Users are considered “New” based on “Behavior learning period”.

If the activities after the Behavior learning period do not intersect with the activities during the Behavior learning period, then that user is considered as a “New” user.

For example, the user activities occurred in the last 24 hours after the Behavior learning period is displayed in the New Users pane. Similarly the user activities occurred in the last 48 hours and 72 hours after the Behavior learning period is...
3. Click a hyperlink in the alphabetical list.

(OR)

Type the search phrase in the search field and then click Search.

EventLogCentral displays the list of users searched for.

4. To do a Log Search, select a row under the Users tab or a row in the first, third, and fourth panes.

EventLogCentral displays the drop-down list.

From the drop-down list, choose Log Search.

5. To view event details in the EventTracker Knowledge Base, select an event id under Event Id column in the first pane.

EventLogCentral displays the drop-down list.

From the drop-down list, choose Knowledge Base.

6. Click the Summary hyperlink to go back to the “Enterprise Activity Summary” page.

---

### Analyzing Activities per System

This option helps you analyze activities occurred at systems. System name is extracted from the Event Properties.

**To analyze activities per system**

- Click a pie on the chart or a legend to view details of activities occurred at the monitored systems.

---

**Top 10 Systems by event count**

- **WEDDOC1** [611,412]
- **NEMO** [53,566]
- **SPIDER** [37,628]

EventLogCentral displays the “Enterprise Activity Detail” page.
Under System Activity tab, sort option, alphabetical list of systems, and search option are provided.

Below that total count of systems monitored and total count of activities are displayed.

Panes on the right-hand side display system activity details.

First pane consists of two parts first displays the event details and the second displays the Weekly trend of events.

Second pane displays top 5 systems by activities. Options are provided to select number of systems and chart type to view.

Third pane displays out of ordinary system activities.

Fourth pane displays new system activities. Systems are considered “New” based on “Behavior learning period”.

Analyzing IP Addresses by Traffic

This option helps you analyze per IP trend of events.
To analyze IP addresses by traffic

IP address is extracted from the Event Description. If the extracted string matches the loopback address ‘127.0.0.1’ or local system IP ‘0.0.0.0’ then it is filtered out. Otherwise, it is considered as a valid IP address.

**Note**

In case of Syslog messages, the extracted string may resemble a valid IP address, which in reality is not. For instance, the version number of file xx.xx.xx.xx matches the pattern searched for but, is not a valid IP.

1. Click a pie on the chart or a legend to view details of activities occurred at the monitored IP addresses.

**Top 10 addresses by occurrence**

- 015.109.166.122 [132]
- 016.109.166.122 [102]
- 009.109.166.122 [58]
- 011.109.166.122 [22]
- 65.55.184.16 [20]
- 018.109.166.122 [18]
- 65.55.200.155 [18]
- 65.55.185.26 [14]
- 216.64.118.251 [13]
- 017.109.166.122 [12]

**Note**

Be patient while EventTracker resolves the IP addresses.

EventLogCentral displays the “Enterprise Activity Detail” page.
Under IPs tab, sort option, total number of IP addresses monitored, and total count of activities per IP are displayed.

Number of records displayed depends upon the “Top activities displayed” criteria you set through the Configuration dialog box.

Panels on the right-hand side display details of activities occurred at monitored IP addresses.

First pane displays the Weekly trend of activities. Host names are displayed, if the IP addresses are resolved, otherwise displayed as “Not available”.

Second pane displays top 5 IP addresses by activities. Options are provided to select number of IP addresses and chart type to view.

Third pane displays out of ordinary IP activities. Helps to monitor abnormal activities by IP addresses and it depends on the “Behavior correlation” criteria you set through the Configuration dialog box.

Fourth pane displays new IP address activities. IP addresses are considered “New” based on “Behavior learning period”.

To do a Log Search, select a row under the IPs tab or a row in the third and fourth panes.

EventLogCentral displays the drop-down list.
From the drop-down list, choose **Log Search**. EventLogCentral opens the Log Search browser with query results.

3 To resolve the IP, click the **Resolve all IPs** hyperlink. EventLogCentral displays the confirmation message box.

![Confirmation message box](image)

4 Click **OK** to proceed further.

5 Click the **Stop** hyperlink to abort the action.

6 To resolve the hostname, click the **Show IP** hyperlink.

7 Click a row under the IPs tab or a row in the third and fourth panes. EventLogCentral displays the drop-down list.

To know who owns the IP, choose **Whois**. EventLogCentral moves you through the DomainTools Web site.

![DomainTools Web Site](image)
Click **Summary** to go back to the “Enterpeise Activity Summary” page.

---

**Analyzing Processes by Occurrence**

This option helps you analyze per user per system process utilization.

**To analyze processes by occurrence**

Events IDs 592 (non-Vista systems) and 4688 (Vista systems) are considered for Process Activity. Information like process name, process id, user name, domain name, and computer name are extracted from the Event Description.

1. Click a pie on the chart or a legend to view process utilization activity details.

![Top 10 Processes by occurrence](image)

EventLogCentral displays the “Enterprise Activity Detail” page.
Under Processes Activity tab, sort option, alphabetical list of processes, and search option are provided.

Below that total count of processes run and total count of activities are displayed.

Summary of per processes utilization is displayed in the list box. Number of records displayed depends upon the “Top activities displayed” criteria you set through the Configuration dialog box.

Panels on the right-hand side display process utilization activity details.

First pane consists of two parts first displays per system per user process utilization details and the second displays the Weekly trend of process utilization activities.

Second pane displays top 5 processes utilized. Options are provided to select number of processes and chart type to view.

Third pane displays out of ordinary process activities. Helps to monitor abnormal process utilization activities and it depends on the “Behavior correlation” criteria you set through the Configuration dialog box.

Fourth pane displays new processes activities. Processes are considered “New” based on “Behavior learning period”.

If the activities after the Behavior learning period do not intersect with the activities during the Behavior learning period, then that user is considered as a “New” process.
For example, the process activities occurred in the last 24 hours after the Behavior learning period is displayed in the New Processes pane. Similarly, the process activities occurred in the last 48 hours and 72 hours after the Behavior learning period is displayed in the New Processes pane. For this, you have to set “Last 2 days” or “Last 3 days” option respectively as Generation Interval.

2. Click a hyperlink in the alphabetical list.
   (OR)
   Type the search phrase in the search field and then click Search.
   EventLogCentral displays the list of users searched for.

3. To do a Log Search, click a row under the Processes tab or a row in the first, third, and fourth panes.
   EventLogCentral displays the drop-down list.
   From the drop-down list, choose Log Search.
   EventLogCentral opens the Log Search browser with query results.

4. Click a row under the Processes tab or a row in the third and fourth panes.
   EventLogCentral displays the drop-down list.
   To know process details, choose What is this?
   EventLogCentral moves you through the ProcessLibrary Web site.

5. Click Summary to go back to the “Enterprise Activity Summary” page.
Analyzing Events by Occurrences

This option helps you analyze events by occurrence.

To analyze events by occurrences

- Click a pie on the chart or a legend to view per event activity details.

EventLogCentral displays the “Enterprise Activity Detail” page.
Under Event ID tab, sort option, total count of events occurred, and total count of activities per event id are displayed.

Panes on the right-hand side display event id activity details.

First pane consists of two parts first displays the event details and the second displays the Weekly trend of events.

Second pane displays top 5 event ids by activities. Options are provided to select number of event ids and chart type to view.

Third pane displays out of ordinary event id activities. Helps to monitor abnormal activities by event ids and it depends on the “Behavior correlation” criteria you set through the Configuration dialog box.

Fourth pane displays new Event Ids activities. Event Ids are considered “New” based on “Behavior learning period”.

Figure 168 Events by occurrence
Chapter 7
Auditing Changes

In this chapter, you will learn how to:

- Audit changes
What is Change Audit

A change audit is a process that helps in identifying voluntary and involuntary changes and developing plans to mitigate the risks.

Prerequisite

You need to have WhatChanged v4.2 b34 installed on the designated EventLogCentral server prior to installing ELC v3.5.

Assessing Changes

This option helps you analyze the summary of Snapshot comparison.

Accessing Changes by Change Type

To assess changes by Change Type

1. Logon to EventLogCentral.
2. Click the Change Audit tab.

EventLogCentral displays the Change Policy Dashboard. By default, EventLogCentral selects the Change Type as View By option.
Note

Change Policy Dashboard displays the summary of snapshot results.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Group</td>
<td>This drop-down list displays all the system groups discovered by the Client Manager</td>
</tr>
<tr>
<td>View Type</td>
<td>Select an option to view chart or data on the console.</td>
</tr>
<tr>
<td>View By</td>
<td></td>
</tr>
<tr>
<td>Authorized</td>
<td>Detected changes that can be matched with an approved change request.</td>
</tr>
<tr>
<td>Unauthorized</td>
<td>Detected changes that cannot be matched to an approved change request.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Configuration audit helps to track all changes that have been made to a computer configuration, or to be able to restore the configuration of that computer back to a known valid restore point.</td>
</tr>
<tr>
<td>Business Knowledge</td>
<td>It is the concept in which an enterprise consciously and comprehensively gathers, organizes, shares, and analyzes its knowledge in terms of resources, documents, and people skills.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files Added</td>
<td>Files Added</td>
</tr>
<tr>
<td>Files Deleted</td>
<td>Files Deleted</td>
</tr>
<tr>
<td>Files Modified</td>
<td>Files Modified</td>
</tr>
<tr>
<td>Registry Added</td>
<td>Registry keys added.</td>
</tr>
<tr>
<td>Registry Deleted</td>
<td>Registry keys deleted.</td>
</tr>
<tr>
<td>Registry Modified</td>
<td>Registry keys modified.</td>
</tr>
</tbody>
</table>

**Change Type Files**

List of files classified under Change Types.

- **Unauthorized**: 
  
  If you wish, you can authorize an unauthorized item.

- **Configuration**: 
  
  *.ini, *.cfg, *.inf, *.nt

- **Business Knowledge**: 
  

- **System**: 
  Files other than the ones listed above are considered as System Change Type.

### Note

File Classification Rules: Administrators can classify files based on content and location so that the files can be more intelligently protected and managed based upon existing business taxonomy. For more information, refer


3 Select the **Data** option from the **View Type** drop-down list.

EventLogCentral displays the Change Policy Dashboard with data.
Click the hyperlinks under Authorized, Unauthorized, Configuration, Business Knowledge, and System to view Change Details.

**Authorizing Unauthorized Items**

This option helps to authorize unauthorized items.

**To authorize unauthorized items**

1. Click the hyperlink under **Unauthorized** column.

   EventLogCentral displays the “Change Details” window.
2. Select an item and then click **Authorize**.

EventLogCentral enables the Save button.

3. Click **Save** to save changes.
EventLogCentral displays the confirmation message box.

Figure 173 Confirmation message box

4 Click OK to continue.

EventLogCentral authorizes and removes the selected item from the list.

Figure 174 Change Details

5 Click Close to close the “Change Details” window.

EventLogCentral authorizes the selected item and lists the count of authorized items under Authorized column.
Viewing Access History

To view access history

1. Click the pie-chart.

EventLogCentral displays the “Change Details” window.
2 Select an item and then click **Access History**. EventLogCentral displays the progress bar.

EventLogCentral displays the Search Access History.
3 Click **Export** to export the report in Excel format. EventLogCentral displays the pop-up window.

4 Click **Save** to save the file.

5 Click **Open** to open the file.
EventLogCentral displays the exported report.

### Viewing More Info on files

To view more info on files

**Note**

You can view more info only for unauthorized items.

- Select an item and then click **More Info**.


### Assessing Changes by Object Type

To assess changes by Object Type

1. Select **Object Type** from the **View By** drop-down list.
EVENTLOGCENTRAL VER. 3.5 USERS GUIDE

CHAPTER 7
AUDITING CHANGES

EventLogCentral displays the Change Policy Dashboard.

![Change Policy Dashboard Image]

2 Select Data from the View Type drop-down list.
EventLogCentral displays the Change Policy Dashboard with data.

![Change Policy Dashboard with Data Image]

3 Click the hyperlinks under Files added, Files deleted, Files modified, Registry added, Registry deleted, and Registry modified columns.
EventLogCentral displays the Change Details.

Assessing Configuration

This option helps to analyze the result of policy comparison.

To analyze policy comparison result

- Click the **Configuration Assessment** hyperlink.

EventLogCentral displays the Policy Comparison Dashboard.
Policies pane displays the Policies that are configured in WhatChanged.

By default, EventLogCentral selects the Dashboard option in the Actions pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Select an option from this drop-down list to view policy comparison details for the selected period.</td>
</tr>
<tr>
<td>Status</td>
<td>Success indicates that the policy was executed successfully on the selected systems and no integrity violations were found. Integrity Violations indicates that the policy was executed successfully on the selected systems and integrity violations were found.</td>
</tr>
<tr>
<td>Title</td>
<td>Name of the policy that was executed on the selected systems. Corresponding details of the selected policy is displayed in the Policy Details pane.</td>
</tr>
<tr>
<td>System</td>
<td>Name of the system against which the policy was executed.</td>
</tr>
<tr>
<td>Generated on</td>
<td>Date and time when the policy was executed.</td>
</tr>
<tr>
<td>Integrity Violation</td>
<td>Count of integrity violations found. If no violations found, then the count is displayed as zero.</td>
</tr>
</tbody>
</table>
**Viewing and Acting on Integrity Violations**

This option helps to mitigate the integrity violations found.

**To view and act on integrity violations**

- Click the hyperlink under the Integrity Violations column.
  
  EventLogCentral displays the details of integrity violations.

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accept</strong></td>
<td>Accept the difference - the master policy is wrong and you know that you have a correct file on your system. Update the master policy with the new file properties.</td>
</tr>
<tr>
<td><strong>Reject</strong></td>
<td>Reject the violation - This generally means that this violation is not important to you. Rejecting it means it is deleted from the master policy.</td>
</tr>
<tr>
<td><strong>Ignore</strong></td>
<td>Ignore the violation for now.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Save the policy with the changes made.</td>
</tr>
</tbody>
</table>
Click **Save As**

To **Save the policy with a new name.**

![Image of the Policy Comparison Dashboard](image)

**Go back to the Policy Comparison Dashboard.**

---

**Scheduling Policy Comparison**

This option helps to schedule policy comparisons against the monitored systems.

**To schedule policy comparison**

1. Click **Scheduled** on the Actions pane.

   EventLogCentral displays the schedule details.

   ![Image of the Scheduled Policy Comparison](image)
2 Click a policy in the Policies pane. EventLogCentral displays the shortcut menu. From the shortcut menu, choose **Scheduled**.

(OR)

Click **New Schedule**.

EventLogCentral displays the “New Schedule” page.
3  Select/enter appropriately in the relevant fields and then click **Save**.
Chapter 8
RSS Feeds

In this chapter, you will learn how to:

- Configure Advanced RSS Feeds
- Add RSS Feeds to the RSS Reader
RSS Feeds

RSS is a simple XML-based system that allows users to subscribe to relevant information within EventLogCentral. Using RSS, the EventLogCentral administrator can put content into a standardized format, which can be viewed and organized through a RSS-aware software. A program known as a feed reader or aggregator can check the list of feeds on behalf of a user and display any updates.

RSS feeds can be configured to be updated on generation of a report. "Advanced Feeds" are those ones visible to all EventLogCentral users. "My Feeds" are specific to user and are only visible to the configured user. While scheduling any "Published", "My Reports" or "Log Analysis" report, users can select any available RSS feed (Advanced Feeds/My Feeds) which will be updated after report generation is complete. An RSS reader on your desktop is used to read feeds periodically and check for updates.

Configuring Advanced Feeds

To configure Advanced Feeds in EventTracker

1. Open the EventTracker Management Console.
2. Click the Configure menu and select the RSS Feeds option. EventTracker displays the RSS Feeds console.
3. Click New Feed. EventTracker displays the “New RSS Feed” window.
4. Type appropriate details in the relevant fields and then click OK.
5. Click Close to close the RSS Feeds console.

Subscribing to RSS Feeds

To subscribe Advanced / My Feeds

1. Log on to EventLogCentral.
2. Click RSS at the right-upper corner.

Had you configured ISA proxy server in your environment, you might encounter error message.
To view RSS Feeds page, do the following.

- Click the **Tools** menu and select the **Internet Options** option.
- Click the **Connections** tab on the Internet Options window.
Figure 191 Internet Options - Connections

- Click LAN settings.
Click Advanced.
Type the IP address of the EventTracker server in the **Exceptions** field.
Click OK.

Click **OK** on the LAN Settings window.

Click **OK** on the Internet Options window.

Refresh the Internet Explorer.

EventLogCentral displays the “EventTracker RSS Feeds” page.
3  Click a link in the “Link” column. IE7 has built-in RSS Reader, which is most commonly used.
Click **Subscribe to this feed** link

Internet Explorer displays the “Subscribe to this feed” dialog box.

![Internet Explorer](image)

Click **Subscribe**.

Internet Explorer successfully subscribes to the feed.

![Internet Explorer](image)
Add RSS feeds in RSS Reader

1. Log on to EventLogCentral.
2. Click the RSS button at the right-upper corner. EventLogCentral displays the RSS Feeds window.
3. Click a link in the Link column.
4. Copy the URL in the address bar.
5. Add the URL in the RSS Reader and then subscribe to the feed. RSS Reader displays the RSS Alert whenever a report linked to the subscribed feed is generated.

Figure 199 RSS Reader
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET framework</td>
<td>The .NET framework created by Microsoft is a software development platform focused on rapid application development, platform independence and network transparency. .NET is Microsoft's strategic initiative for server and desktop development for the next decade. According to Microsoft, .NET includes many technologies that are designed to facilitate rapid development of Internet and intranet applications.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>The directory service environment for Microsoft Windows 2000 (and later) servers. Active Directory includes enough information about users, groups, organizational units and other kinds of management domains and administrative information about a network to represent a complete digital model of the network.</td>
</tr>
<tr>
<td>Alerts</td>
<td>A feature that instructs programs that notify timely information about the events</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>In Windows NT and Windows 2000 networking, the domain controller (DC) is the server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain. It is the server that essentially makes networking (at least in a secure function) possible.</td>
</tr>
<tr>
<td>Event Analysis</td>
<td>Process of analyzing the event details by setting criteria such as date range, time range, rule, and computer</td>
</tr>
<tr>
<td>Event Knowledge</td>
<td>The database that contains information about Windows events and custom EventTracker events. You can view events information through Knowledge Base Web site</td>
</tr>
<tr>
<td>ELC</td>
<td>Web based user interface of EventTracker.</td>
</tr>
<tr>
<td>EventTracker</td>
<td>An application that can be used to centrally monitor, analyze, manage events being emitted by Windows NT/2000/XP, UNIX systems, and SNMP enabled devices.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>A web site containing information about Windows events and custom EventTracker events.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>http</td>
<td>The Hypertext Transfer Protocol is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.</td>
</tr>
<tr>
<td>https</td>
<td>A TCP/IP protocol that is used by World Wide Web servers and Web browsers to transfer and display hypermedia documents securely across the Internet.</td>
</tr>
<tr>
<td>IIS</td>
<td>Microsoft's Web server that runs on Windows NT platforms. IIS comes bundled with Windows NT 4.0; Because IIS is tightly integrated with the operating system, it is relatively easy to administer.</td>
</tr>
<tr>
<td>My Reports</td>
<td>My Reports are exclusively available for the users who created it.</td>
</tr>
<tr>
<td>On Demand Report</td>
<td>On Demand Reports can be run at any time. The configuration settings cannot be saved but the generated output can be saved in a computer.</td>
</tr>
<tr>
<td>Published Reports</td>
<td>Advanced reports published by EventTracker. These reports are available for all the logged in users. Published Reports can be configured in both EventTracker as well as EventTracker.</td>
</tr>
<tr>
<td>Runaway Process</td>
<td>Occasionally a process will stop responding to the system and run wild. These processes ignore their scheduling priority and insist on taking up 100% of the CPU. Because other processes can only get limited access to the CPU, the machine begins to run very slowly.</td>
</tr>
<tr>
<td>Service</td>
<td>A program that can be automatically started as part of the operating system start-up process and that runs continuously in the background. Specific information about the program and its configuration is recorded in the operating system's registry. It's this configuration information that identifies the program and turns it into a service. Services can be manipulated using the Services MMC snap-in (e.g. in Computer Management) or by the sc command.</td>
</tr>
</tbody>
</table>

A service may require other services to operate; in this case, the first service is said to be dependent on the other services. If a depended upon service isn't running or cannot be started, the service(s) that are dependent won't start either. For example, the Print Spooler service is dependent on the Remote Procedure Call service.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session</td>
<td>A session is either a lasting connection using the session layer of a network protocol or a lasting connection between a user (or user agent) and a peer, typically a server, usually involving the exchange of many packets between the user's computer and the server. A session is typically implemented as a layer in a network protocol (e.g., telnet or FTP).</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator, an HTTP address used by the World Wide Web to specify a certain site. This is the unique identifier, or address, of a web page on the internet.</td>
</tr>
</tbody>
</table>
Index

A
Access
  shortcuts ........................................ 23
Alerts
  analysis ........................................ 178
  notification .................................... 181
Alphabetical .................................. 82

C
Collection Points
  CAB info......................................... 22
  switching ........................................ 20
Configuring
  advanced feeds ........................... 238
  my feeds ........................................ 90
  reports ........................................... 96
Cost Saving .................................. 189
  person hour .................................... 189
Custom ...... 133, 134, 135, 143, 150,
  151, 155, 159, 163, 165, 170
  time range .................................... 41
Custom Column ............................. 133
  components ................................. 135
  display name ................................ 135
  need ............................................. 134
  occurrences ................................. 135
  prior knowledge ............................ 135
  separator ...................................... 136
  terminator ..................................... 136
  what is ........................................ 135
Customize Logo ............................ 23

D
Defined .......................................... 126, 168
Detail........................... 136, 154, 162, 168

E
ELC
  configuring .................................... 24
  exiting ......................................... 46
  starting........................................ 13
  upgrading .................................... 45
ELC Home .................................... 76
ELC Icons .................................... 20
ELC User Groups
  ELC Administrator Group.................... 13
  EventTracker .................................... 13
E-mail ......................................... 98, 109
Event-O-Meter ......................... 19
Exceptions .................................... 93
Favorites........................................ 130
  adding ......................................... 130
  viewing ........................................ 130
IP Address .................................... 171
  resolving ...................................... 175
License Exceeded ......................... 18
Log Analysis
  detail .......................................... 136, 154, 162, 168
  summary ....................................... 147, 157, 164
  trend ............................................ 151, 160, 167
Log Search .................................... 28
  advanced ....................................... 135
  basic ........................................... 136
Log Volume .................................... 182

O
On Demand 110, 114, 116, 119, 122,
  125, 136, 147, 151, 178, 182, 187
  foreground .................................... 116
  power viewer .................................. 119
  queued ........................................ 125
smart viewer ................................ 122

Port Details ................................ 171
Prerequisites ................................ 13

Queued ...... 115, 125, 154, 157, 160, 177, 179, 184, 187

Refine and Filter ................................ 98
Reg-ex ............................................ 132
Regular Expression .......................... 132
Report Snapshot ............................. 85, 88
Reports
  configuration ................................ 96
  exceptions ..................................... 93
  wizard ......................................... 93
Reports Dashboard ............................ 83
Roles ............................................. 52
  adding ......................................... 63
  assigning ...................................... 56
  changing ....................................... 61
  deleting ........................................ 69
  editing ......................................... 67
  permissions ................................... 52
  privileges ..................................... 52
  user information ............................. 53

RSS Feeds
  advanced ..................................... 89
  my feeds ....................................... 90
  subscribing .................................... 238

Scheduled .... 99, 107, 110, 162, 164, 167, 180, 185, 188
Scheduled Reports
  configuring .................................... 99
  history ........................................ 107
  on demand ..................................... 110
Session
duration ...................................... 25
SMTP ............................................. 98
Standard .... 136, 147, 151, 154, 157, 160, 162, 164, 167, 168
Starting ELC .................................... 13
Summary ...... 77, 147, 157, 164, 177
Suspicious Traffic ............................ 186

Use Configuration ......................... 100, 137
User
  permissions ................................... 54
User Authentication .......................... 13
Users
  deleting ....................................... 72
  report ......................................... 55
  unassigned ................................... 55